L'Economia del Corriere della Sera
27-NOV-2017
pagina 2
foglio 1 / 4

SENTIRSI AL SICURO

CYBER LADRI IN AZIONE: ITALIA VULNERABILE

di **Ferruccio de Bortoli**

2

CYBER LADRI ITALIA SENZA RETE

Il nostro Paese è all'undicesimo posto nella classifica della capacità di proteggersi dagli attacchi informatici. Ma siamo tra quelli meno preparati nel gestire i «rapimenti» di dati sensibili che si concludono con richieste di riscatto. Le aziende, spesso piccole, sono molto internazionali eppure inclini a sottovalutare il rischio

In Europa il 75% dei board non ha esperti tech, da noi anche meno: in futuro saranno indispensabili L'indifferenza, giustificata con l'idea che non verranno a cercare proprio noi nella vastità del web, va di pari passo con la poca attenzione agli aggiornamenti e alla segregazione dei sistemi Dal 2018 sarà obbligatorio denunciare eventuali hackeraggi. Ma ci vorrebbe un piano di difesa nazionale

Un terzo dei dirigenti globali ha ammesso di essere stato colpito da virus (dati Kroll)

La legge 626 del 1994 che norma la sicurezza nei posti di lavoro andrebbe adeguata a questi temi

di **Ferruccio de Bortoli**

Pochi giorni fa, in un seminario organizzato dagli studenti dell'Università Bocconi, si discuteva dei pregi (pochi) e dei difetti (molti) della classe dirigente italiana. Marianna Vintiadis, head of Southern Europe di Kroll, la più grande società al mondo nella sicurezza informatica, non è andata tanto per il sottile nel definire l'inspiegabile, a suo giudizio, miopia dell'attuale establishment italiano. E soprattutto del mondo industriale. «Sapete qual è la cosa che più mi stupisce oggi?». L'attenzione degli studenti è salita di colpo. «La totale sottovalutazione da parte delle aziende dei pericoli informatici, degli attacchi cibernetici. E, guardate bene, non è una questione tecnologica, ma soprattutto culturale. E i media non ne parlano o ne parlano poco o male...».

Sfrondato il tema dagli ovvii interessi societari di Kroll, rimane un interrogativo di fondo che vale la pena di approfondire. La struttura industriale italiana è fatta soprattutto di piccole e medie aziende, nelle quali l'attenzione alla trasformazione digitale — assai elevata almeno nelle migliori — non va di pari passo con quella della difesa di dati, informazioni e brevetti.

Battaglie

E come se, di fronte allo scatenarsi di guerre planetarie che vedono in gioco gli interessi delle grandi potenze, scattasse nell'imprenditore il seguente ragionamento minimalista. Perché mai queste organizzazioni così potenti e ramificate, magari impegnate nel deviare il corso delle democrazie, a occuparsi di armi, spionaggio, droga, dovrebbero dedicare attenzione a quello che accade in uno sperduto capannone della Brianza o in un laboratorio emiliano? E qui sta l'errore colossale, la svista

colpevole. La convinzione pericolosa che si possa essere leader mondiali nel proprio specifico settore di attività e, nello stesso tempo, mimetizzarsi perfettamente, passare inosservati. Emergere sul proprio mercato di riferimento e nascondersi come entità sensibile nella Rete. Se si riflette ancora un attimo, questa tendenza non è altro che la proiezione su scala aziendale di quella che è una predisposizione personale dell'utente normale assai poco preoccupato di che fine facciano i propri dati personali. Ma il danno per un'azienda anche piccola può essere irreparabile. E non è subito visibile.

La mappa

La malavita digitale è dappertutto. La soglia di ingresso nel cyber crimine è relativamente bassa. La disponibilità di talenti perversi pressoché infinita. Lo spionaggio industriale in alcuni Paesi, dalla Cina alla Russia e non solo, è addirittura considerato una missione nazionale, una questione di bandiera. Se non si rispettano brevetti e modelli nella realtà industriale, fisica, è assai difficile che ciò avvenga in Rete, dove diritti e protezioni, in una dimensione virtuale, sono ancora meno tutelati. Nel più recente Global Securities Fraud Risk Report di Kroll è descritta la tipologia degli attacchi informatici e le relative difese. Un terzo dei dirigenti intervistati, a livello mondiale, ha ammesso di aver ricevuto attacchi sotto forma di virus o worm. Seguono le incursioni phishing tramite mail. Un quarto dichiara di aver subìto cancellazioni gravi di dati. Nella mappa globale del rischio, l'Italia è tra i Paesi più esposti anche come conseguenza del grado di internazionalizzazione dell'economia e del successo dei suoi prodotti su vari mercati. Ma è tra i meno consapevoli dei rischi che corre il suo apparato industriale e produttivo ed è privo di una strategia efficace di difesa nazionale. Forse perché solo dal prossimo anno vi sarà un obbligo di dichiarare gli eventuali hackeraggi subiti. Obbligo che esiste anche attualmente, se solo si gestiscono dati di clienti americani.

La classifica

Secondo il Security Index, elaborato da Accenture, l'Italia è undicesima nella capacità di proteggersi dagli attacchi informatici. Siamo però tra i meno preparati nell'evitare ed eventualmente nel gestire le azioni di ransomware, ovvero le incursioni che si risolvono con il pagamento di un «riscatto» in denaro. Ed è più frequente, rispetto alle statistiche estere, che a mettere in atto gli attacchi, o ad esserne complici, siano ex dipendenti e collaboratori. A livello europeo, il 75 per cento dei board non ha nemmeno un membro con competenza in materia informatica. In Italia ancora meno. Eppure una quota di esperti prima o poi sarà addirittura indispensabile.

«Episodi di questo genere avvengono pressoché ogni giorno — spiega Vintiadis — quasi un bollettino di guerra sul quale, e mi domando perché, vi sia tutto questo silenzio. Noi notiamo che l'imprenditore preferisce spesso pagare e stare zitto, molti non hanno misure di back up, l'aggiornamento dei sistemi è decisivo ma avviene ancora con troppa lentezza». Nei casi recenti più clamorosi — come per esempio il cosiddetto Wannacry che ha interessato 300 mila computer di 150 Paesi e messo in crisi il sistema ospedaliero britannico (Nhs) — la falla che ha agevolato le incursioni degli hacker è stata proprio la disattenzione nell'aggiornamento dei sistemi. E qualcosa di analogo è avvenuto quando Mosca, in un attacco informatico contro l'Ucraina, ha danneggiato diversi gruppi internazionali come Maersk e Wpp. La mancata segregazione dei sistemi è un fattore di estrema debolezza. Unicredit ha denunciato, tra il giugno del 2016 e il luglio del 2017, incursioni che hanno riguardato, senza conseguenze, 400 mila conti e portato a rafforzare i presidi di sicurezza. Non si sarebbe trattato di un vero e proprio attacco di hacker, bensì di una sottrazione di dati attraverso una società di cessione del quinto alla quale era stato consentito, forse con una certa leggerezza, l'accesso al sistema.

I raggiri

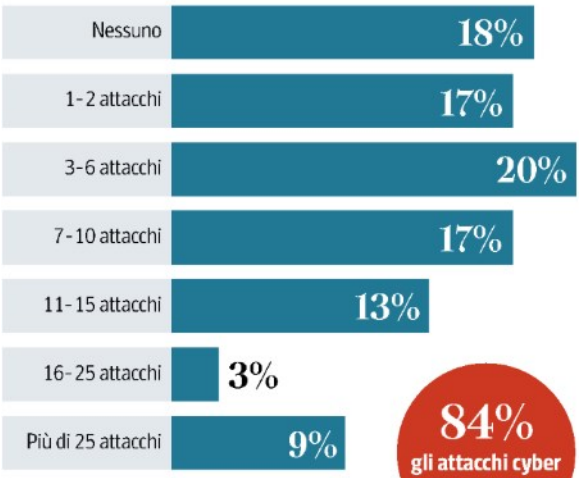
In molte altre circostanze ci troviamo di fronte a schemi consueti, ai più classici dei raggiri. La mail o il colpo di telefono al funzionario che è indotto a fare in fretta un bonifico, com'è avvenuto per gli uffici confindustriali a Bruxelles. «Basterebbe — spiega Carola Frediani autrice di

Guerre di Rete (Laterza) — avere un po' più di conoscenza del problema e attuare minime azioni di cautela nell'uso della posta elettronica, nel non impiegare sempre la stessa password, nel non aprire allegati sospetti, nel disabilitare le macro nel file di Office per ridurre i rischi più evidenti. Ma il vero pericolo è quello delle incursioni silenti nei sistemi. Operazioni che violano proprietà intellettuali e sottraggono informazioni sensibili. A qualsiasi livello, aziendale o governativo, le modalità non cambiano».

Il nemico in casa senza accorgersene. E qui emerge tutta la fragilità italiana. Si oscilla tra il fatalismo digitale e l'adesione fideistica all'ultimo sistema. Un affidarsi totale agli esperti, quasi sempre esterni, senza preoccuparsi troppo della crescita aziendale di una cultura della prevenzione. La legge 626 del 1994 sulla sicurezza sui posti di lavoro forse andrebbe aggiornata anche in questa direzione.

Pericoli diffusi

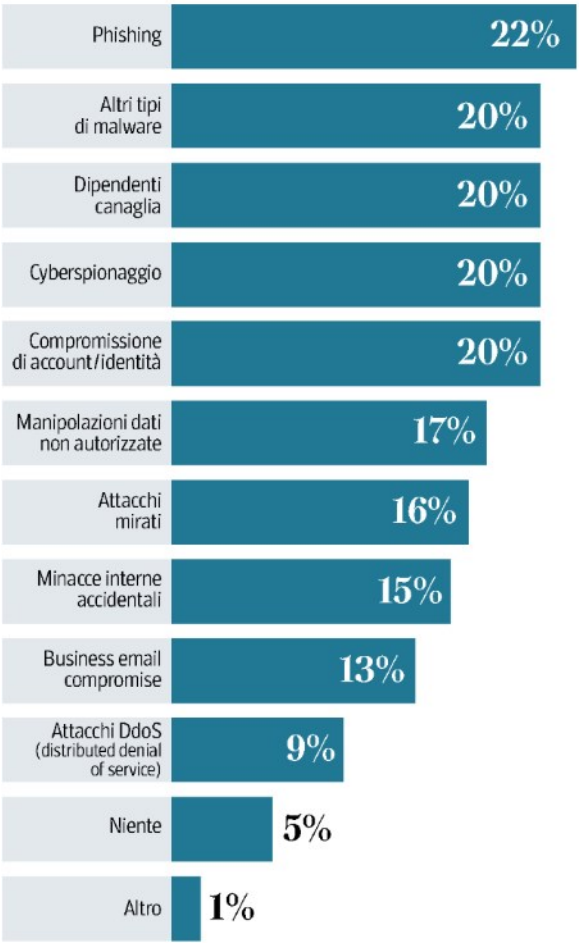
Il numero di attacchi cyber che le aziende italiane hanno dovuto affrontare nell'ultimo anno



84% gli attacchi cyber ransomware

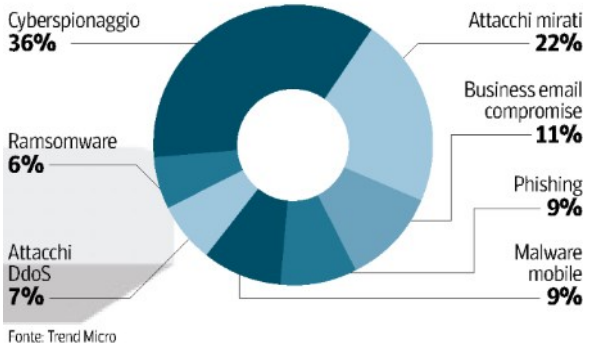
La mappa

Le minacce alla sicurezza di altro genere affrontate lo scorso anno



I timori

Gli attacchi alla sicurezza dell'azienda che preoccupano di più per i prossimi 12 mesi



Fonte: Trend Micro