LA STAGIONE DELLA CYBER-INSICUREZZA

di GIACOMO CORVI

IL RISCHIO INFORMATICO SI CONFERMA COME UNA DELLE PRINCIPALI MINACCE PER IMPRESE E CITTADINI IN ITALIA, MA A OGGI RISULTANO ANCORA POCO DEFINITE LE ADEGUATE MISURE DI PROTEZIONE. SECONDO GABRIELE FAGGIOLI, PRESIDENTE DEL CLUSIT, È NECESSARIO ACCRESCERE LA CULTURA DIGITALE NEL NOSTRO PAESE, LE COMPETENZE E LA CAPACITÀ DI AGGIORNARE COSTANTEMENTE I SISTEMI DI SICUREZZA AZIENDALE

Il fenomeno del cyber risk si fa sempre più diffuso e pervasivo. E ogni anno si rivela l'occasione buona per aggiornare qualche record negativo. È stato così anche nel 2022, almeno secondo l'ultima edizione dell'ormai tradizionale rapporto curato dal **Clusit**. Anzi, per usare proprio le stesse parole dell'associazione italiana per la sicurezza informatica, il 2022 è stato "l'anno peggiore di sempre per la cyber security". Il numero di attacchi informatici di grave entità divenuti di dominio pubblico ha infatti raggiunto lo scorso anno il nuovo massimo storico di 2.489 incidenti in tutto il mondo, dato in crescita del 21% su base annua. Il 44% degli episodi ha avuto una gravità definita elevata, il 36% addirittura critica.

"Sono numeri che purtroppo non destano grande sorpresa", esordisce **Gabriele Faggioli**, presidente del Clusit. "Il fenomeno del cyber risk, almeno per come analizzato dalla nostra associazione, registra ormai da anni – prosegue – un trend di crescita piuttosto lineare, con tassi di variazione annuale che oscillano fra il 10% e il 20%, certamente dettati anche in parte dallo sviluppo tecnologico della società, che ha allargato la superficie di attacco a disposizione di hacker e criminali del web, nonché dai nuovi obblighi di *disclosure* imposti alle imprese dalla normativa vigente, cosa che ha consentito di incrementare la trasparenza del mercato e di far emergere episodi che magari in passato, per paura di ripercussioni negative, potevano essere tenuti nascosti". Il risultato è che negli ultimi cinque anni il numero di attacchi gravi è cresciuto del 60% a livello globale. Peccato però che a questo progressivo aumento non sia corrisposto un adeguato incremento delle misure di sicurezza. E che tutto ciò abbia contribuito ad allargare un gap di protezione che il rapporto del Clusit arriva a definire "cyber-insicurezza".

L'ITALIA NEL MIRINO

Insomma, la situazione non è delle migliori e in Italia sembra essere addirittura peggiore. Il rapporto del Clusit fotografa in poche parole lo scenario della sicurezza informatica del nostro paese: anche l'Italia è ormai del mirino di hacker e criminali informatici. La ricerca, a tal proposito, evidenzia che lo scorso anno si sono verificati nel nostro paese 188 attacchi cyber di grave entità divenuti di pubblico dominio, dato che evidenzia un balzo del 169% su base annua.

***Gabriele Faggioli**, presidente del Clusit*

"Sono numeri che non rispecchiano l'evoluzione del cyber risk a livello globale e che non possono trovare giustificazione nel normale sviluppo del fenomeno", riflette Faggioli. "L'Italia rappresenta il 2,2% del Pil mondiale, eppure – aggiunge – nel 2022 gli attacchi informatici avvenuti nel nostro paese sono stati pari al 7,6% del totale registrato in tutto il mondo, una percentuale che è del tutto incredibile". Tutto ciò, a detta di Faggioli, è sintomatico di "un paese che è strutturalmente fragile, che non si è mai dotato di adeguate misure di sicurezza e protezione e che pertanto può diventare, ed è di fatto ormai diventato, un facile bersaglio per criminali del web che, come del resto avviene anche nella vita reale, tendono ad attaccare chi ha uno scarso livello di protezione".

COMPETENZE SCARSE...

Alla base di questa situazione c'è anche quella che Faggioli non tarda a definire "una vergogna nazionale". L'Italia, spiega l'esperto, "ha una scarsissima cultura digitale: secondo il rapporto *Desi* (*Digital Economy and Society Index*, ndr) della Commissione Europea, è terzultima per competenze digitali e ultima assoluta per laureati in discipline Stem".

Per Faggioli, "è una situazione inaccettabile su cui è necessario che tutte le istituzioni intervengano per colmare il gap di competenze e porre le basi per un assetto più adeguato alla minaccia informatica che imprese e privati cittadini si ritrovano oggi ad affrontare". Anche perché, prosegue, "basterebbe poco per evitare errori grossolani o disattenzioni che possono provocare danni enormi al nostro tessuto sociale e produttivo: un dipendente adeguatamente formato sulla portata del cyber risk, per esempio, potrebbe evitare di cliccare su link malevoli o scaricare allegati arrivati per posta elettronica che poi diffondono un virus sui server aziendali e bloccano le funzionalità informatiche della società per cui lavora".

... E POCHI INVESTIMENTI

A voler trovare del buono in qualsiasi cosa, si può almeno dire che la consapevolezza delle imprese è aumentata parecchio in questi anni. "La sempre più ampia diffusione di notizie di attacchi informatici a società, aziende e istituzioni ha avuto, se non altro, il merito di veicolare la portata del cyber risk alle imprese", riflette Faggioli. "L'*Osservatorio Cybersecurity & Data Protection* del **Politecnico di Milano**, di cui sono responsabile scientifico, ci dice che da due anni il cyber risk è al primo posto nell'agenda delle grandi aziende e delle piccole e medie imprese". Peccato però che solo raramente questa consapevolezza si traduca in investimenti efficaci per la gestione del rischio informatico. "Lo stesso osservatorio – prosegue Faggioli – ha evidenziato che l'Italia ha speso nel 2022 poco meno di due miliardi di euro, pari allo 0,1% del Pil, in sicurezza informatica, mentre in altri paesi del G7 si è arrivati a spendere il doppio in termini di percentuale sul Pil, in alcuni casi addirittura il triplo sempre in termini di percentuale sul Pil: è una differenza enorme, che scava un solco sempre più profondo fra l'Italia e le altre economie avanzate del mondo".

Secondo l'esperto, le maggiori difficoltà risiedono soprattutto nelle piccole e medie imprese, in quell'enorme tessuto di aziende familiari, studi professionali e liberi professionisti che magari fatturato qualche decina di milioni di euro all'anno e che, pertanto, non hanno forse nemmeno le capacità finanziarie per dotarsi autonomamente di un'efficace sistema di sicurezza informatica. "Qualche investimento è stato fatto in questi ultimi anni, ma tanti piccoli investimenti non bastano a creare una rete di protezione diffusa", osserva Faggioli. "A ciò – prosegue – si aggiunge poi il fatto che non è sufficiente un intervento *una tantum* per garantire la sicurezza di cui un'azienda oggi ha bisogno: la tecnologia evolve e, con lei, evolve anche il rischio informatico, quindi è fondamentale tenere aggiornati costantemente i propri sistemi di sicurezza".

INSIEME CONTRO IL RISCHIO INFORMATICO

Resta però il fatto che in uno scenario di risorse scarse, come quello che caratterizza il tessuto produttivo in Italia, può risultare difficile dotarsi di un efficace sistema di sicurezza informatica. Ecco allora che per

© Tero Vesalainen - iStock

© Sitthiphong - iStock

Faggioli la parola d'ordine diventa una sola: aggregazione. "Credo che sia arrivato il momento che le aziende prendano pienamente consapevolezza del rischio e delle risorse necessarie a gestirlo e che, sulla base di questa comprensione, capiscano anche l'importanza di unirsi per poter sfruttare la leva delle economie di scala e garantire in questo modo a tutti la protezione di cui abbiamo bisogno", afferma.
In alternativa (o in aggiunta), Faggioli sottolinea poi la necessità di "affidarsi a grandi player del settore per la gestione dei sistemi informatici aziendali, almeno di quelli che magari non costituiscono il core business dell'impresa: sono grandi operatori di mercato che dispongono già delle risorse necessarie per sfruttare le economie di scala e che vantano competenze adeguate alla portata del rischio che stiamo affrontando".

NELLE MANI DELLA CRIMINALITÀ ORGANIZZATA

A incentivare la necessità di un intervento che si fa sempre più urgente per garantire la sicurezza informatica di imprese e cittadini, c'è poi l'evoluzione di un fenomeno che sembra andare più veloce della fantasia e dell'immaginazione. Se ne è avuto prova anche di recente. Prima con la pandemia di coronavirus che, con la forte spinta impressa alla digitalizzazione, ha prestato il fianco ad hacker e criminali del web. E poi, più recentemente, con la guerra in Ucraina, che ha reso il dominio digitale un nuovo e, per certi versi, inedito campo di battaglia.
Secondo Faggioli, nel prossimo futuro, l'attenzione dovrà essere rivolta soprattutto verso la grande criminalità organizzata. "Già oggi il cosiddetto *cybercrime* è una delle cause principali di attacchi informatici, e credo che nel futuro lo sarà ancora di più", afferma. "Il ritorno d'investimento del crimine informatico, considerando anche l'alto livello di impunità che caratterizza in fenomeno, è di gran lunga superiore a molte altre attività criminali: magari in Italia, in un contesto caratterizzato da tante piccole e medie imprese, non sarà possibile portarsi a casa un bottino milionario, però la ricompensa per i criminali del web può essere comunque ingente".

L'OFFERTA ASSICURATIVA CHE VERRÀ

Il rischio zero per imprese e cittadini non potrà mai esistere nel dominio informatico. Ed è qui, secondo Faggioli, che deve inserirsi l'offerta assicurativa. "Ci troviamo un po' a un momento di passaggio: da un lato, ci sono sempre più aziende che si rivolgono alle imprese del settore per valutare la possibilità di sottoscrivere una polizza assicurativa e, dall'altro, alcune compagnie, almeno sulla base di quello che leggiamo sulla stampa specialistica, hanno preso la decisione di uscire dal mercato", afferma. Secondo l'esperto, "è una dinamica del tutto comprensibile: la minaccia informatica è un rischio ancora relativamente nuovo, su cui non ci sono forse ancora abbastanza dati e informazioni per delineare in sicurezza tutti i termini di una polizza, quindi non mi sorprende che alcune compagnie abbiano deciso di lasciare almeno momentaneamente questo mercato".
Molto, a detta di Faggioli, dipenderà anche dalle capacità del cliente di misurare e gestire il rischio all'interno della propria azienda. "È inevitabile trovarsi di fronte a polizze piene di esclusioni o dal costo esorbitante se prima non si è fatto nulla per gestire autonomamente il rischio", osserva. "Ci vorrà magari ancora del tempo, ma sono sicuro – conclude – che in futuro ci sarà spazio per un mercato di questo genere e per soluzioni adeguate alle richieste dei clienti".