UNA SCARSA COMPRENSIONE DEL FENOMENO

di GIACOMO CORVI

CLIENTI POCO INFORMATI E CONDIZIONI DI POLIZZA ANCORA NEBULOSE: È QUESTO, SECONDO GABRIELE FAGGIOLI, PRESIDENTE DEL CLUSIT, CHE STA IMPEDENDO LO SVILUPPO DI UN MERCATO MATURO DELLE COPERTURE ASSICURATIVE IN MATERIA DI RISCHIO INFORMATICO. INTANTO IL FENOMENO CRESCE: GLI ATTACCHI CYBER SARANNO IN FUTURO SEMPRE PIÙ FREQUENTI

La multinazionale della farmaceutica **Merck** è stata una delle principali vittime dell'attacco cyber passato alle cronache con il nome di *NotPetya*. Partito il 27 giugno 2017 in Ucraina, il virus ha inizialmente contagiato un server della sede locale del colosso statunitense, propagandosi poi sul resto della rete e bloccando buona parte dei dati inseriti all'interno del sistema: per la loro liberazione, come in ogni attacco ransomware che si rispetti, era stato chiesto un riscatto di 300 dollari in Bitcoin per ogni singolo computer che era stato infettato.
Secondo un'accurata ricostruzione di *Bloomberg*, pubblicata lo scorso dicembre, l'attacco avrebbe colpito complessivamente 30 mila computer e 7.500 server della società. Interi settori industriali, come la produzione di vaccini, restarono a lungo bloccati. Il risultato per la multinazionale fu una perdita stimata in 1,3 miliardi di dollari. Di fronte a un disastro di simili proporzioni, Merck fece quello che avrebbe fatto chiunque: presentò il conto ai propri assicuratori, forte di una serie di polizze che aveva sottoscritto nel corso degli anni contro rischi catastrofali per un massimale complessivo di 1,75 miliardi di dollari. O almeno così credeva. Le compagnie coinvolte si sono infatti rifiutate di indennizzare il sinistro: l'attacco cyber è stato compiuto dalla **Gru**, un'agenzia di intelligence russa, e costituisce pertanto un atto di guerra, fattispecie specificatamente esclusa nelle condizioni di polizza sottoscritte dalla multinazionale.

RISCHIO INFORMATICO, QUESTO SCONOSCIUTO

La questione, come ricostruisce l'agenzia di stampa statunitense, è finita in tribunale. E costituisce per **Gabriele Faggioli**, presidente del **Clusit** e responsabile scientifico dell'*Osservatorio information security & privacy* del **Politecnico di Milano**, la cartina di tornasole di una delle principali criticità del mercato delle polizze cyber: i clienti spesso non sanno quello che sottoscrivono. "Gli assicurati hanno raramente una chiara comprensione di quello che firmano e, allo stesso tempo, le stesse compagnie non sembrano avere una piena percezione del rischio che può derivare da un attacco cyber", afferma in questa intervista a *Insurance Review*. "Servono polizze più chiare – prosegue – capaci di dire in maniera immediatamente comprensibile cosa viene coperto e cosa invece resta escluso".
La scarsa comprensione del fenomeno resta uno degli ostacoli principali allo sviluppo di un mercato assicurativo maturo. Secondo un'indagine condotta dall'osservatorio su un campione di 166 imprese italiane, il 64% delle aziende riscontra difficoltà nella misurazione degli impatti finanziari che un attacco cyber può avere sul proprio business, un altro 58% lamenta l'incapacità di valutare correttamente l'esposizione al rischio, e il 19% denuncia la scarsa competenza tecnica di assicuratori e broker.

UN MERCATO PICCOLO MA IN CRESCITA

Poste queste basi, non stupisce che il mercato delle polizze cyber in Italia risulti ancora asfittico. Sempre secondo i risultati della stessa indagine, appena il 33% delle imprese ha sottoscritto una qualche forma di copertura contro questo genere di rischio: il 25% del campione afferma di essere in fase di valutazione, il 30% ha scartato completamente l'ipotesi e il restante 12%, più candidamente, ammette di non conoscere minimamente

IMPRESE E POLIZZE CYBER

Fonte: *Osservatorio Security & Privacy del Politecnico di Milano*

IL CONTRIBUTO DELLA NORMATIVA

Il *Gdpr* e il *Cybersecurity Act* a livello europeo, il recente decreto sulla sicurezza informatica a livello nazionale: negli ultimi anni si sta facendo molto sentire il contributo del legislatore in materia di cyber risk. "Si tratta di un tema ormai normativamente affrontato e la direzione appare positiva", commenta Gabriele Faggioli, presidente del Clusit e responsabile scientifico dell'Osservatorio information security & privacy del Politecnico di Milano. "Avere dei framework nazionali, creare dei collegamenti a livello sovranazionale e aumentare la capacità di acquisire nuove conoscenze – prosegue – è sicuramente condivisibile e potrà avere ripercussioni positive sui modelli che il mercato deciderà di adottare per affrontare il rischio informatico".

l'argomento. "Come già accennato – riflette Faggioli – ci sono difficoltà nel comprendere la propria esposizione al rischio e, sull'altro fronte, c'è un'offerta di mercato che non viene considerata ancora all'altezza della situazione: le polizze appaiono confuse, poco chiare, non tarate sulle specifiche esigenze delle aziende e incapaci di coprire adeguatamente i rischi".
Nonostante tutto, le prospettive del settore restano comunque positive. "Il mercato delle polizze cyber è destinato sicuramente a evolvere", confida Faggioli. "Siamo ancora in una fase di immaturità – aggiunge – ma è inevitabile che assisteremo a una crescita del settore, vedremo quanto velocemente".

ATTACCHI CYBER IN AUMENTO

Alla base delle previsioni di crescita c'è principalmente l'idea che anche il rischio cyber pare destinato a un forte aumento. E ciò, secondo Faggioli, in ragione di "un motivo molto semplice: sta crescendo in maniera esponenziale l'uso delle tecnologie e, di conseguenza, aumenterà anche la possibilità per organizzazioni criminali di lanciare attacchi che possono avere ritorni economici rilevanti". I numeri, già oggi, non sembrano lasciare spazio a dubbi. Nei primi sei mesi del 2019, secondo l'ultimo rapporto del Clusit, si sono contati ben 757 attacchi cyber gravi a livello globale, in crescita dell'1,3% rispetto allo stesso periodo dell'anno precedente. Il cyber-crime si conferma la principale causa di attacco (85%), mentre restano stabili le intrusioni a fini di spionaggio (11%) e di guerra informatica (2%).
"È difficile dire che forma prenderà il fenomeno nel prossimo futuro, ma certamente assisteremo a un'ulteriore crescita", afferma Faggioli. La speranza è che anche gli investimenti in sicurezza informatica possano andare nella stessa direzione. "Servono maggiori stanziamenti in tecnologia e formazione del personale", aggiunge, auspicando che l'attenzione sul tema, anche sulla scia di una pressione mediatica che si sta facendo sempre più forte, possa aumentare. "Persino la vicenda di Merck – conclude con una punta di ottimismo – può rivelarsi alla fine un'occasione per costruire un rapporto più sano, chiaro, diretto e coerente fra imprese e compagnie assicurative".