CYBER, OGNI IMPRESA HA IL SUO RISCHIO

IL MERCATO DELLE COPERTURE DI CYBERSICUREZZA È IN CRESCITA COSTANTE, ANCHE SE LA PENETRAZIONE SI AGGIRA ANCORA SUL 5%, E LE PRINCIPALI SPINTE ALL'ACQUISTO DI POLIZZE SONO CORRELATE AI DIVERSI OBBLIGHI NORMATIVI E A OPPORTUNITÀ DI FILIERA. SUL FRONTE DELLE COMPAGNIE, LA PROPOSTA E I SERVIZI CONNESSI SI STANNO AFFINANDO E SONO ALLO STUDIO GARANZIE SUI DANNI MATERIALI E SUI RISCHI INFORMATICI LEGATI ALL'AI

di Maria Moro

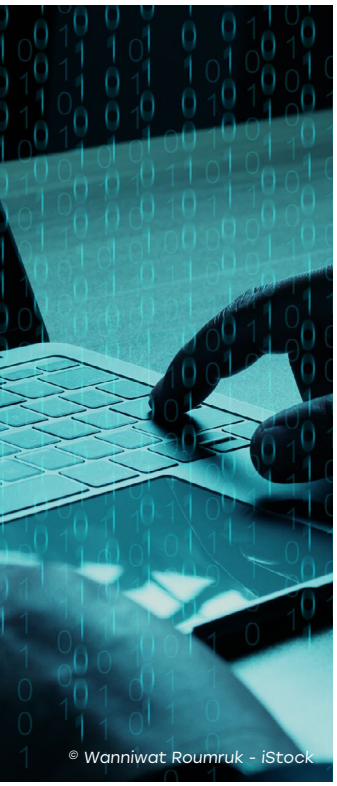
La crescita del mercato delle coperture cyber è stata la risposta concreta a una sensibilità sul rischio tecnologico che negli ultimi dieci anni sta progressivamente crescendo tra le imprese, incluse quelle piccole e medie. Le minacce si sono intensificate e le aziende le hanno sentite avvicinare attraverso casi riportati dalla cronaca o vivendole più o meno direttamente. La stessa valorizzazione strategica delle tecnologie e il loro ruolo determinante per l'operatività quotidiana hanno portato il tema sui tavoli dei consigli di amministrazione e indotto a programmare attività e destinare budget per la gestione del rischio cyber.

Tra le ragioni che portano le imprese italiane a lavorare sulla cyber sicurezza e a sottoscrivere una polizza assicurativa ce ne sono anche altre: gli obblighi normativi, gli standard richiesti dai clienti della filiera, le questioni reputazionali.

"Incontriamo sempre più spesso aziende che sottoscrivono una copertura cyber per adempiere a una richiesta contrattuale, ma va detto che è concreta la preoccupazione dell'impatto che un attacco cyber può avere sull'operatività, provocando un blocco o un'interruzione parziale dell'attività caratteristica", afferma **Rossella Bollini**, head of cyber di **Marsh Italia**. Il movente normativo è reale e prioritario per le imprese: "attraverso prima il Gdpr e poi Nis2, AI Act e Dora, l'intento dei regolatori è di spingere le aziende a costruire la loro resilienza e attraverso questa creare una resilienza dell'intero sistema, prosegue Bollini. Nis2, ad esempio, si rivolge alle imprese strategiche facendo una distinzione tra i soggetti essenziali (le infrastrutture) e i soggetti importanti, ovvero i non critici. Stabilisce, inoltre, che la filiera stessa debba rispondere a requisiti di sicurezza molto rigidi, allargando in questo modo il coinvolgimento al sistema economico del Paese. "Dal nostro punto di vista – afferma Bollini – la Nis2 sarà un driver per l'aumento della domanda, con un processo graduale ma significativo".

ESIGENZE DIVERSE TRA AZIENDE PICCOLE E MEDIE

Da un certo punto di vista, quindi, le imprese sono tutte ugualmente interessate dal rischio cyber, indipendentemente dalla dimensione, ma in realtà una differenza in termini di consapevolezza si nota. Fatto salvo che le grandi realtà da


© Wanniwat Roumruk - iStock

tempo hanno alzato il livello di controllo e adottato contromisure, tra medie e piccole il divario si allarga. “In Italia il segmento Pmi è generalmente sottoassicurato e le coperture cyber hanno un tasso di penetrazione appena del 5%. Tuttavia – osserva Bollini – esistono differenze tra le piccole e le medie imprese, innanzitutto rispetto alle risorse e agli investimenti in sicurezza informatica. In genere i budget per questo rischio sono circoscritti, ma la differenza viene fatta soprattutto dalla capacità della media impresa di avere un approccio strutturato, con un piano di risk management, budget per la sicurezza informatica, risorse dedicate, piani di emergenza, formazione. Per le piccole realtà le risorse sono limitate e spesso il rischio cyber residuo viene gestito con il patrimonio aziendale, senza trasferimento al mercato assicurativo. Notiamo un processo di evoluzione in questo senso, ma ci vuole tempo”.

DUE VIE PARALLELE: PREVENZIONE E RESILIENZA

Nella gestione del rischio cyber, la consapevolezza è il primo passo; da qui le imprese iniziano a mettere in atto misure di prevenzione e possono decidere di trasferire il rischio residuo al mercato assicurativo: tutto questo si colloca all’interno di un processo di revisione che deve essere continuo, in risposta all’evoluzione delle minacce, e che determina la capacità dell’organizzazione di essere resiliente.

In termini di prevenzione il focus è sull’adozione di soluzioni tecnologiche, ma è altrettanto necessario influire sulle persone. Bollini ricorda che il cosiddetto fattore umano è tra le cause più ricorrenti di incidenti cyber o di frode via social engineering, e rappresenta uno dei volti del rischio più difficili da presidiare: “governare l’elemento fattore umano – sottolinea – è complesso, perché sfugge agli investimenti del presidio tecnologico e rientra nell’ambito della cultura aziendale. La formazione del personale è qualcosa su cui è opportuno investire in modo mirato, con training profilati sui ruoli specifici e sulla seniority. È questo un punto che portiamo costantemente all’attenzione dei nostri clienti”.

Arrivare a essere resilienti significa, come visto, fare un passo in più dall’operatività della prevenzione alla strategia nella gestione del rischio. Su questo punto il comparto assicurativo può dare un grande supporto alle Pmi. “La componente di gestione della crisi – spiega la head of cyber di Marsh Italia – è un asset importante del prodotto assicurativo, che può aiutare le imprese a garantire l’operatività quotidiana in caso di incidente cyber, ad esempio con misure di *incident response* e con l’intervento tempestivo di esperti di *IT forensic* o di team legali. Registriamo però delle differenze nelle esigenze dei clienti legate alla loro dimensione e struttura. Se l’azienda piccola predilige il ruolo attivo dell’assicuratore, con i suoi servizi, nella gestione dell’evento cyber, le medie imprese mostrano un interesse meno spiccato per gli aspetti operativi e più orientato al trasferimento del rischio. Le grandi imprese, in genere, non considerano la componente di servizio offerta dalle compagnie e preferiscono cercare capitali importanti sul mercato assicurativo per trasferire il rischio di severità, meno quello di frequenza”.

L’OFFERTA DEL MERCATO ASSICURATIVO

Il mercato assicurativo cyber è giovane e ha tassi di crescita significativi. Oggi si mostra dinamico, caratterizzato da forte competitività e dall’ingresso di nuovi attori che negli ultimi due anni hanno portato una nuova capacità assuntiva. “Dopo la fase di irrigidimento del periodo 2018-2021, il mercato è più favorevole al cliente, gli appetiti delle compagnie si sono ampliati, così come la portata delle garanzie, inoltre la competizione non si basa solo sul pricing ma guarda alla portata delle coperture”, commenta Bollini. Le previsioni sulle dinamiche di mercato sono quindi per la permanenza di uno stadio competitivo (al netto di eventi cyber molto gravi) ma caratterizzato da volatilità. Anche la proposta ha avuto un’evoluzione significativa: “le coperture sono molto aggiornate, è cambiato l’approccio assuntivo e le soluzioni si mostrano più sofisticate, declinate sulla tipologia di rischio secondo la dimensione dell’azienda cliente. Tuttavia, c’è molto che si può fare”. Un’area poco esplorata ma di grande importanza per le imprese è il danno materiale da evento cyber, su cui al momento ci sono soluzioni limitate che provengono dal mercato anglosassone; un altro ambito importante allo studio del mercato riguarda i rischi cyber legati all’AI. “Come osservatori – conclude Bollini – riteniamo che i prodotti assicurativi si svilupperanno verso questi due ambiti”.