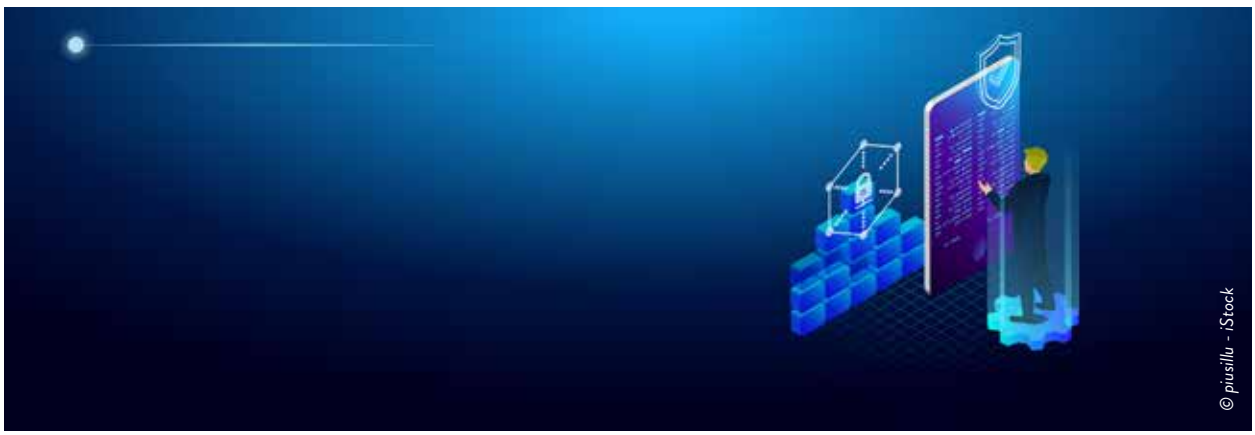
# ALLARME CYBER RISK: NON È ASSICURABILE

di FABRIZIO AURILIA

I DANNI GLOBALI DERIVANTI DAL RISCHIO INFORMATICO AMMONTANO A CIRCA 945 MILIARDI DI DOLLARI, MA CIRCA IL 90% DELLE PERDITE RESTA, A OGGI, NON ASSICURATO. SWISS RE CONSIGLIA DI PUNTARE SU RISK MANAGEMENT, NUOVE TECNOLOGIE E COLLABORAZIONE TRA GLI STAKEHOLDER DEL SETTORE




Secondo **Swiss Re**, gli attacchi informatici sono "sempre più gravi e sofisticati", e gli hacker utilizzano tecniche di estorsione sempre più evolute, mentre la diffusione dei ransomware ha abbassato le barriere di ingresso per i criminali informatici. La crescente digitalizzazione rende le infrastrutture sempre più vulnerabili, con ricadute che arrivano fino all'interruzione di servizi essenziali come fornitura di acqua, energia o rete internet.

"L'aumento degli attacchi informatici ha elevato la consapevolezza dei rischi che si corrono e quindi la domanda di protezione assicurativa in ambito cyber, ma per la difficile quantificazione delle potenziali perdite, e per via di uno scenario in rapida evoluzione, il rischio informatico ha un'assicurabilità limitata. Questo restringe la capacità del mercato, con un gap di protezione in ambito cyber che è intorno al 90%".

A dirlo è **Jérôme Haegeli**, capo economista di Swiss Re, presentando il nuovo studio del riassicuratore globale sul rischio informatico, e richiamando la necessità di un nuovo approccio delle assicurazioni.

## IL GAP TRA I PREMI E LE PERDITE

Guardando al rapporto, è evidente l'aumento della frequenza e della gravità degli attacchi cyber: due elementi che hanno spinto la crescita del mercato, con premi assicurativi globali che nel 2021 potrebbero raggiungere i 10 miliardi di dollari. Le previsioni parlano, inoltre, di una crescita annua del 20% fino al 2025, fino a raggiungere un ammontare complessivo

di 23 miliardi di dollari. Tuttavia, dicono gli analisti, "considerando che i danni globali derivanti dal rischio cyber ammontano a circa 945 miliardi di dollari, circa il 90% delle perdite rimarrebbe non assicurato".
Nonostante la rapida crescita, i premi rimangono, quindi, una frazione delle perdite annuali e questo gap è dovuto ad alcuni limiti di assicurabilità per questo specifico tipo di rischio. "A causa dell'interconnessione dell'economia – spiega Swiss Re – ogni singolo attacco può potenzialmente avere impatti sull'intero portafoglio di un riassicuratore, con danni di tipo sistemico la cui copertura sarebbe insostenibile".

## L'EPOCA DEI RANSOMWARE

Il settore assicurativo ha comunque un ruolo chiave in tre ambiti: migliorare l'uso dei dati e dei modelli, aumentare la coerenza e la chiarezza dei contratti, individuare nuove fonti di capitale.
Prima del virus *NotPetya*, del 2017, i rischi informatici erano incentrati soprattutto sulle violazioni dei dati e sulla responsabilità verso terzi. Per i riassicuratori, la proliferazione delle normative sulla privacy dei dati ha aperto le porte a procedure di contenzioso e ha aumentato l'esposizione al rischio a coda lunga (*long tail risk*). Negli ultimi due anni, invece, i sinistri puri sono diventati dominanti, con l'esplosione di ransomware da parte della criminalità organizzata, che hanno spostato i danni al core business.

### SANITÀ SOTTO ASSEDIO

Uno dei settori divenuti ormai chiave per l'assicurazione è la sanità. Il numero di *data breach* nel comparto sanitario, si legge nel rapporto di Swiss Re, sta crescendo in linea con altri settori ad alta intensità di dati, con le strutture più piccole che emergono come i bersagli preferiti dei criminali informatici.
Negli Stati Uniti, il 2021 è stato un anno record per le violazioni segnalate da enti sanitari. Come per le Pmi in generale, gli attacchi informatici hanno un impatto relativo maggiore sulle strutture più piccole, con capacità informatiche inferiori. L'anno scorso, il 75% delle violazioni dei dati ha riguardato sinistri in cui sono stati coinvolti meno di 30mila individui. Gli attacchi che hanno coinvolto oltre 1,5 milioni di persone sono stati meno dell'1% del totale.


© anyaberkut - iStock

Le imprese, i riassicuratori, le associazioni di settore e le autorità pubbliche hanno moltiplicato gli sforzi di gestione del rischio e hanno collaborato per fornire non solo il trasferimento, ma anche la mitigazione della minaccia cyber, contribuendo a monitorare gli attacchi informatici.

## LA NATURA UMANA DEL CYBER RISK

Ma il divario di protezione, come si diceva, rimane ampio. In una recente ricerca è emerso che solo il 55% delle aziende ha dichiarato di avere una copertura contro il cyber risk e meno di una su cinque ha limiti di copertura superiori alle necessità per i danni da ransomware. Gli analisti hanno stimato che il costo totale di un incidente informatico che colpisce una Pmi è, in termini relativi, tre volte superiore a quello di una grande azienda, con costi legali che generalmente vanno dai 20mila ai 100mila dollari per una società con un fatturato inferiore ai 50 milioni.
Secondo Swiss Re, c'è spazio per considerare nuove opportunità per meccanismi di condivisione del rischio pubblico-privato. "Queste misure – si legge nel report – possono aiutare a mitigare le esposizioni complessive, migliorare la comprensione dei rischi e contribuire a rendere le società più resilienti agli attacchi, evitando conseguenze devastanti e potenzialmente sistemiche".
La natura umana e di rete del cyber risk fa pensare che le minacce evolveranno continuamente e richiederanno una risposta coordinata: "il miglioramento della resilienza – concludono gli analisti – richiederà la collaborazione tra società, (ri)assicuratori e governi".