CYBER RISK, LE POSSIBILI RISPOSTE DEGLI ASSICURATORI

di FEDERICO CASINI
ceo di Howden Italia

Negli ultimi anni il cyber risk è cresciuto esponenzialmente tanto da mettere in estrema difficoltà le aziende e costringere gli assicuratori a trovare delle contromisure.
I sempre più frequenti attacchi informatici, da parte di hacker individuali così come di organizzazioni criminali internazionali, da un lato hanno reso l'assicurazione cyber una priorità per aziende piccole e grandi; dall'altro spingono molte compagnie a intervenire sui premi e sulle condizioni per ridurre i rischi.
Il risultato è stato quello di creare un potenziale corto-circuito che lascia alcune aziende senza copertura, e alcune compagnie alle prese con enormi perdite.

Le dimensioni del fenomeno

Oggi il mercato assicurativo cyber globale conta circa 10 miliardi di dollari in premi raccolti, con una crescita stimata a 25 miliardi entro il 2025.
Il Global Insurance Market Index ha rilevato che nel secondo trimestre 2022 i prezzi delle assicurazioni cyber sono cresciuti mediamente del 79% negli Stati Uniti e del 68% nel Regno Unito, dopo un aumento rispettivamente del 110% e del 102% nel trimestre precedente.

Dall'inizio della pandemia, si è registrato un incremento esponenziale di cyber-attacchi, in particolare ransomware, con un costo medio di 4,35 milioni di dollari per le aziende che li hanno subiti. In media sono stati necessari dai 9 ai 12 mesi per identificare e contenere le conseguenze dannose di questi incidenti.

I criminali informatici possono essere in grado di accedere ai sistemi di un'azienda, esfiltrare i dati e lanciare un attacco ransomware a distanza di tempo o decidere di vendere i dati sul dark web; tutto questo in un'epoca nella quale il valore dei dati è in continuo aumento.

Dai piani di back up all'education in azienda

Per fortuna gli operatori del mercato si sono già attivati per mettere a punto le opportune contromisure, e gli incrementi delle polizze sembrano essere vicini alla stabilizzazione.
Le compagnie propongono sempre più un approccio consulenziale volto alla prevenzione dell'incidente piuttosto che all'indennizzo ex post: più dettagliata l'analisi delle vulnerabilità e più solide le pratiche di utilizzo dei sistemi richieste agli utenti.

Si valutano positivamente, non solo pratiche di back up dei dati e piani di risposta rapida agli incidenti per ripristinare le operazioni in seguito a un attacco, ma anche l'attenzione all'education della forza lavoro sul tema cyber security.
D'altro canto, le aziende sono sempre più consapevoli dell'importanza di una formazione continua per far fronte a rischi cyber sempre nuovi e più sofisticati.
Perché si evitino incidenti in azienda, spesso dovuti a inconsapevolezza o disattenzione, è in primis necessario che gli utenti siano convinti dell'utilità dei protocolli di sicurezza e che siano consapevoli che l'implementazione di questi non va a scapito dell'efficienza operativa. Il tempo e le risorse investiti in questa direzione sia organizzativa che culturale sono più che mai ben spesi.
Fortunatamente, è in costante crescita il numero di aziende che adottano misure anti-ransomware, definiscono robusti controlli di sicurezza o piani di risposta agli incidenti e sono disposte ad approfondire le proprie architetture di cybersecurity.


© Chainarong Prasertthai - iStock

Una soluzione di assessment e riduzione del rischio

Un altro aspetto da tenere in considerazione è l'importanza di una collaborazione sempre più stretta tra mondo assicurativo, cyber-tecnico e legale.
*Tanto per fare un esempio, il gruppo di cui sono ceo in Italia, **Howden**, uno dei maggiori player mondiali del brokeraggio, insieme con **Yoroi**, società specializzata nella cybersecurity, parte del gruppo **Tinexta**, hanno lanciato recentemente una soluzione innovativa per ridurre il rischio cyber nel* merger & acquisition*, realizzata con l'assistenza legale di **Dla Piper**.*
Il nuovo prodotto consente di valutare con rapidità e precisione l'esposizione potenziale al rischio cyber di aziende oggetto di fusione/acquisizione, di adottare soluzioni correttive e di ottenere un'idonea copertura assicurativa all'altezza delle aspettative degli attori coinvolti nell'operazione; il tutto in linea con le sfidanti tempistiche di questo genere di transazioni.
Del resto, anche società target di operazioni di M&A possono essere bersagli inconsapevoli di un attacco informatico, che potrebbe manifestarsi solo dopo il closing dell'acquisizione. Come dimostrano alcuni casi recenti che hanno ricevuto una notevole copertura mediatica, le conseguenze dannose possono essere anche molto significative.
In questo caso, l'unione di tre leader di mercato nei rispettivi settori, ha consentito di ottenere una soluzione di assessment e riduzione del rischio che non esisteva nella cornice internazionale dell'M&A, tramite un prodotto 'chiavi in mano' con tempi di implementazione rapidi e perfettamente in linea con le stringenti tempistiche di operazioni di fusione/acquisizione.
Il gruppo Howden sta studiando inoltre nuove soluzioni su misura per particolari situazioni di cyber risk anche in altre aree di mercato, a dimostrazione della forza e del dinamismo del settore assicurativo, pronto più che mai a cercare alleanze e a trovare le contromisure più idonee per far fronte alle nuove sfide.