Cyber Risk, assicurare è meglio che curare: come gestire il rischio informatico

Secondo il World Economic Forum (WEF), nel 2019 gli attacchi cyber si posizionano tra i primi 5 scenari di rischio con più alta probabilità di accadimento. Ma niente paura: se è vero che non è possibile prevenire totalmente un attacco cyber, è anche vero che **le polizze per il cyber risk possono essere un'ancora di salvezza per le aziende** che vogliono limitarne l'impatto.

Cos'è il rischio cyber e perché è importante gestirlo?

Le minacce alla Cyber Security sono ormai riconosciute come uno degli scenari più gravi in termini di impatto sul business. Tuttavia, anche se le azioni messe in campo dalle aziende sono in aumento, in molti casi non sono presenti standard condivisi o non si compiono sforzi per quantificare il rischio.

> Ma che **cosa si intende per cyber risk**? Secondo l'Institute of Risk Management, par cyber risk o rischio informatico si fa riferimento a qualsiasi **rischio di perdita finanziaria, distruzione o danno alla reputazione di un'organizzazione** dovuta ad un malfunzionamento del sistema informativo.

Come se già questa definizione non fosse abbastanza allarmante, gli attacchi cyber sono al 7° posto nella classifica del WEF che valuta la gravità degli impatti derivanti da questa tipologia di evento. Questo significa che **il cyber risk è un rischio concreto che può colpire le imprese in diverse forme**, perciò deve essere affrontato in maniera sistematica e con una strategia ben definita. A tal fine, occorre **considerare il rischio cyber valutando sia le tecnologie, sia la noncuranza (volontaria o meno) dei dipendenti**, causa numero uno della vulnerabilità informatica nelle imprese.

Come gestire il rischio cyber: il processo di Cyber Risk Management

La gestione del rischio cyber è articolata in un **processo mirato a individuare le vulnerabilità del sistema informativo**, le possibili minacce e i potenziali danni di una violazione della sicurezza. Questo processo può essere **suddiviso in 5 fasi.**

1. **Identificazione dei rischi:** individuazione delle possibili fonti e degli scenari di rischio cyber che possono colpire l'azienda;
2. **Classificazione e stima dei rischi**: valutazione delle due componenti di rischio – probabilità di accadimento (frequenza con la quale si presuppone che un dato evento possa verificarsi) e gravità/impatto (severità delle conseguenze causate dallo scenario di rischio);
3. **Valutazione dei rischi**: confronto la tra possibilità di accadimento del rischio e i criteri di appetibilità definiti dall'impresa, al fine di capire la rilevanza dei rischi per l'organizzazione;
4. **Trattamento e mitigazione dei rischi**: pianificazione e attuazione di misure per modificare le due componenti di rischio in modo che rientri nei parametri di sostenibilità aziendali;
5. **Trasferimento del rischio**: ricorso a polizze di cyber risk insurance per trasferire a terze parti il rischio residuo.

Il Cyber Risk Management nella pratica

Quali azioni compiono le aziende italiane nel concreto? Ponendo l'attenzione sul processo di **assessment del rischio cyber**, il 77% delle aziende conduce *penetration test* e *vulnerability assessment*, in modo da valutare la gravità delle vulnerabilità di un sistema ed evidenziare come queste potrebbero compromettere la sicurezza. Il 46% considera in fase di assessment sia le tecnologie sia i dipendenti, mentre il 27% effettua periodicamente valutazioni dei fornitori.

Per quanto riguarda la **mitigazione dei rischi**, si ricorre a questa metodologia soprattutto per la protezione degli endpoint, delle applicazioni e dei dati personali di clienti e dipendenti.

Invece, per il **trasferimento del rischio** le aziende ricorrono a **polizze di cyber risk** per assicurarsi contro la perdita di dati personali di clienti, dati finanziari e di reputazione.

Le polizze di Cyber Risk Insurance

Dopo la fase di mitigazione dei rischi permane il cosiddetto rischio residuo. Qualora esso sia superiore al limite del *risk appetite* aziendale, è possibile ricorrere ad una polizza di cyber insurance per trasferire il rischio.

In risposta alla crescente attenzione da parte delle aziende verso il tema della sicurezza informatica, sta crescendo anche l'offerta del mercato assicurativo. Infatti, il mercato delle assicurazioni cyber offre diverse opzioni di copertura riguardanti la perdita o la diffusione di dati sensibili. Non solo, è possibile tutelarsi anche dai danni derivanti da una compromissione del sistema informativo o da un'interruzione del servizio.

A livello concreto, con una polizza di cyber insurance si può, per esempio, coprire il mancato guadagno dovuto all'interruzione di un'attività, le eventuali spese di consulenza nella gestione della crisi, le spese legali, i danni causati da un'estorsione e i danni causati a terzi a seguito di una perdita di dati.

Il mercato della Cyber Security Insurance in Italia

Il tema della cyber risk insurance è già fortemente radicato a livello internazionale, mentre in Italia si tratta di un mercato in crescita ma ancora agli albori. Secondo i dati della Survey 2018 dell'Osservatorio Information Security & Privacy, lo stato dell'arte del mercato è il seguente:

- Il 18% delle aziende del campione ha attivato una polizza specifica per il cyber risk;
- Il 15% ha optato per una copertura generalista che copre in parte il rischio cyber;
- Il 25% è in fase di valutazione;
- Il 30% è a conoscenza delle possibilità di copertura ma non è intenzionato ad adottarne una;
- Il 12% confessa di non essere a conoscenza della possibilità di stipulare una polizza per il rischio cyber.

Gli ostacoli che stanno rallentando la crescita del mercato assicurativo sono molteplici. Si tratta di una questione culturale ma non solo. Va sicuramente considerata l'oggettiva difficoltà nella misurazione degli impatti finanziari derivanti da un eventuale incidente di sicurezza, insieme all'incapacità di valutare correttamente l'esposizione ai rischi cyber. Ci sono poi limiti tecnologici e organizzativi, ma anche problemi legati alla scarsa trasparenza delle stesse assicurazioni cyber.