CYBER, STRETTA CONNESSIONE CON I PROCESSI DI ERM

di MARIA MORO

L'EVOLUZIONE E LA TRASVERSALITÀ DELLA MINACCIA TECNOLOGICA NEL CONTESTO AZIENDALE IMPONGONO UN'ATTIVITÀ DI RISK MANAGEMENT SECONDO TEMPI E CRITERI DIFFERENTI RISPETTO AGLI ALTRI RISCHI OPERATIVI. UNA DELLE MAGGIORI CRITICITÀ RIGUARDA IL RAPPORTO CON LA SUPPLY CHAIN, MA IN CASO DI ATTACCO VA POSTA ATTENZIONE ALLA RELAZIONE CON LE ALTRE CATEGORIE DI RISCHIO AZIENDALE

Il primo passo per affrontare la minaccia cyber è prendere coscienza della sua reale pervasività nell'operatività aziendale: se i sistemi tecnologici sono la spina dorsale di ogni attività, il rischio connesso è una presenza potenziale che va sempre considerata, con l'aggravante di essere in costante evoluzione sia nelle forme conosciute che in nuove manifestazioni. L'aleatorietà di un rischio impalpabile, difficilmente comprensibile fino a quando non si manifesta, rappresenta il primo vero ostacolo nella sua gestione, tanto nelle forme più conosciute quanto nelle potenziali minacce che possono emergere da un contesto in evoluzione. Anche nelle organizzazioni più strutturate e in cui è attivo un sistema di *enterprise risk management*, la gestione del rischio cyber parte da un approccio molto differente rispetto agli altri.

Una tavola rotonda organizzata da **Anra**, lo scorso 4 maggio a Milano, ha provato ad analizzare le caratteristiche del rischio cyber per comprendere come si possa raccordare con il processo di enterprise risk management e quali possano essere le conseguenze per l'impresa in caso di violazione della sua sicurezza informatica.

La minaccia tecnologica è una costante articolata e mutevole, che presenta complessità nel momento in cui si intende gestirla. "Affrontare il rischio cyber richiede esperienza e conoscenze specifiche, necessarie a comprendere come i sistemi operano e quali sono le loro vulnerabilità; in più si inserisce in un contesto che cambia continuamente, caratterizzato dal profilarsi di minacce sempre nuove e dalla vulnerabilità data dall'interdipendenza con partner esterni", ha sintetizzato in apertura dei lavori **Paola Radaelli**, vicepresidente di Anra e senior risk management consultant di **Strategica Group**.

VALUTARE LE CONSEGUENZE AD AMPIO SPETTRO

Anche per il rischio cyber il punto di partenza deve essere l'analisi dello scenario, sia quello generale che quello, più ristretto, in cui si muove l'azienda. È il caso dell'attuale contesto di guerra, che ha messo in moto meccanismi di *cyber war* da un lato imprevedibili nei loro impatti, dall'altro portatori di innovazione nei sistemi di attacco che potrebbero trovare presto pure un uso "civile", ad esempio in nuove forme di ransomware. Nel contesto più limitato dell'attività aziendale il rischio tecnologico va valutato sempre, ad esempio nel momento in cui si decidono di affrontare nuovi domini di business che possono presentare delle vulnerabilità. Un aspetto fondamentale per **Carlo Zaganelli**, responsabile enterprise risk management di **Leonardo**, è mantenere "un approccio guidato dalla componente di *forward looking*, perché nella valutazione delle minacce future fare tesoro delle esperienze pregresse può aiutare solo in maniera limitata". Se il risk mana-

ger affianca i *process owner* in tutte le fasi dell'attività aziendale, dalla pianificazione della strategia fino all'approdo al mercato e al post vendita, la componente cyber non deve fare eccezione. "Come risk manager abbiamo l'obbligo di far vedere l'intero spettro degli impatti che possono derivare da una minaccia cyber. Questi nell'immediato riguarderanno la continuità operativa e in parallelo pure la *compliance*, laddove il mancato rispetto del profilo normativo, che è molto stringente, porta con sé sanzioni dal peso economico non trascurabile. Da qui è immediato il riflesso sulla reputazione, fondamentale per l'esistenza dell'azienda sul mercato e chiave della sua sostenibilità nel medio - lungo periodo".

Il rischio cyber non può prescindere dalla governance della catena del valore di un'impresa. L'attenzione si sposta quindi al ruolo delle Pmi come parte della supply chain di un'impresa più strutturata, la quale potrà gestire meglio i propri rischi, inclusi quelli tecnologici, se saprà supportare i propri fornitori e clienti nella realizzazione di un governo del loro rischio, creando se possibile un'integrazione a tutela reciproca dalle minacce.

LA CRITICITÀ DELLA VARIANTE TEMPORALE

Esperienza, conoscenza tecnica, competenze peculiari, rendono necessario uno specifico presidio di cyber security, funzione che dovrà interagire con quella di enterprise risk management. Secondo **Luca Bechelli**, partner information & cyber security di **P4I**, questa relazione necessaria trova nella gestione temporale il principale punto critico: "Il presidio dei rischi operativi richiede di ragionare con una visione a medio termine, dai 3-5 anni fino ai 10, mentre la supervisione del rischio cyber richiede un'osservazione costante e continuata, su tempistiche di pochi mesi in risposta a minacce che evolvono rapidamente sia per come si manifestano sia negli effetti che producono. Per fare un esempio, cinque anni fa l'intelligenza artificiale aveva un ruolo limitato nella sicurezza cyber, oggi creare una difesa contro malware e ransomware senza considerare questa tecnologia rappresenta quasi una vulnerabilità. Allo stesso modo, valutare i rischi di una piattaforma da qui a cinque anni è impresa velleitaria". La gestione del rischio cyber ha come colonne portanti le tempistiche brevi, la capacità di reazione, il riconoscimento della complessità e i costi, tutti aspetti che richiedono di avere una rapidità decisionale che non ha paragoni con gli altri rischi.

Questa visione include il rapporto con la supply chain e la possibilità di coinvolgerla nella gestione del rischio. Le grandi aziende puntano a condividere le informazioni per costruire un presidio dei rischi, ma nelle valutazioni va considerato che ciò richiederebbe un'impostazione *by design* descrivibile in un accordo, quando la continua evoluzione del rischio può rapidamente renderlo obsoleto.

MEGLIO NON CEDERE AL RICATTO

Sempre in un'ottica di gestione del rischio aziendale, la minaccia cyber porta con sé una serie di altre criticità che vanno attentamente soppesate a priori e che riguardano i rischi operativi, i rischi economico-finanziari, etici e di reputazione, oltre che assicurativi. **Sonia Peron**, presidente del collegio sindacale di **Garofalo Health Care** e revisore di Anra, mette in guardia rispetto alla scelta di pagare il riscatto in caso di attacco ransomware. Nonostante la normativa, l'azienda che si vede sequestrare i dati potrebbe pensare di coprire l'evento per tutelare la propria reputazione, "questo però fa incorrere in condotte vietate dal d. Lgs. 231/01 sulla responsabilità amministrativa degli enti, configurando i reati di false comunicazioni sociali o di ostacolo all'esercizio delle funzioni dell'autorità di vigilanza, possono verificarsi i casi di impedito controllo, di autoriciclaggio, di finanziamento della criminalità organizzata".

In questo contesto, la copertura assicurativa rimane una soluzione che **Giulio Coraggio**, head of intellectual property & technology, **Dla Piper Partner**, definisce "necessaria ma non esaustiva" rispetto alla tutela dalla minaccia cyber e che ricorda essere sempre soggetta a un'attività preliminare di valutazione del rischio da parte della compagnia di assicurazioni.