IL SOLE 24 ORE – 22 OTTOBRE 2024

La cybersecurity è una priorità per il management

di Greta Nasi

Oggi le organizzazioni sono sempre più digitali, sviluppano prodotti e servizi con processi automatizzati e interagiscono con utenti e clienti con strumenti come le chatbots attraverso canali digitali. Diversi studi, come il rapporto Assintel e quello dell'Osservatorio Digital Innovation del Politecnico di Milano, mostrano l'aumento degli investimenti informatici, segnalando come la trasformazione digitale sia una priorità rilevante della strategia di aziende, all'attenzione dei Consigli di amministrazione. L'uso pervasivo delle tecnologie nelle organizzazioni genera dipendenza. Tale situazione, inevitabilmente, espone le aziende ad un ventaglio di rischi connessi ad eventuali attacchi cyber o incidenti informatici, come quello recente di Crowdstrike, i cui potenziali impatti sono di assoluta gravità: si pensi alle interruzioni dei processi e del funzionamento aziendale, e ai collegati potenziali mancati ritorni economici, o a danni reputazionali; situazione che, a cascata, generano ulteriori effetti negativi sulla filiera e l'intero sistema produttivo.

I vertici aziendali e i consigli di amministrazione valutano e approvano, attraverso attente analisi di dati, gli investimenti tecnologici per ottimizzazione i costi di produzione e aumentare il valore generato, mentre la sicurezza informatica viene ancora troppo spesso considerata come un problema esclusivamente tecnico. Le conseguenze negative di interruzioni temporanee o prolungate dei sistemi informatici sono misurate come costo operativo di ripristino e come costi derivanti dall'interruzione delle attività, così sottostimando gli effetti sulla sostenibilità economica, la perdita di proprietà intellettuale e di fiducia da parte dei clienti. In tal modo non si definisce adeguatamente il ruolo che la sicurezza informatica dovrebbe avere tra le priorità dei vertici di ogni realtà aziendale, comprese

quelle di medio/piccole dimensioni che, attraverso la filiera automatizzata, sono connesse alle aziende di più grandi dimensioni.

Purtroppo, però, è difficile trovare dati oggettivi che supportino e diano evidenza degli effetti a lungo periodo di un attacco o di un incidente informatico e ciò in quanto non vengono misurati (o resi noti) i reali impatti sulla performance aziendale, nella filiera di produzione e sul sistema paese. Tale opacità sulla magnitudo degli effetti del «rischio cyber» finisce per allontanare il problema dall'attenzione dei vertici.

Data la natura delle minacce odierne, i Consigli di amministrazione e i comitati direttivi hanno il dovere di garantire che le misure di sicurezza siano adeguate e che l'azienda sia preparata a rispondere a un eventuale attacco. La Direttiva Europea NIS 2 che l'Italia ha recepito con il D.Lgs. 138/2024 con lo scopo di rafforzare la sicurezza delle reti e dei sistemi informatici, conferma che il Consiglio di Amministrazione e il Ceo debbano possedere le conoscenze e le competenze necessarie per valutare i rischi legati alla cybersecurity. Tali competenze devono essere anche estese all'Organismo di Vigilanza, a cui la legge 90 del 2024 in materia di cybersicurezza ha attribuito un ruolo centrale per monitorare il rispetto delle misure di tutela stabilite dall'Autorità per la Cybersicurezza Nazionale (ACN).

Questi sono passi importanti per strutturare una governance per la cybersecurity che coinvolga i vertici aziendali la quale, tuttavia, per essere efficace deve sfociare in azioni concrete e rafforzative messe in atto dalle aziende. Per fare ciò è necessario fornire ai vertici analisi oggettive sugli impatti economici e non economici di attacchi o incidenti informatici, in modo da portare l'attenzione sui temi di loro competenza, dando informazioni complete e trasparenti, necessarie per le decisioni da prendere. In secondo luogo, è opportuno integrare i sistemi interni di controllo gestione del rischio in ottica multidimensionale, integrando i rischi finanziari, quelli non finanziari e quelli cyber in modo tale da fornire una loro mappatura completa. Ciò richiede un investimento in competenze di cybersicurezza con una prospettiva non solo tecnica ma anche economica e manageriale in grado di

leggere i benefici della trasformazione digitale, analizzarne i rischi e supportare decisioni per l'economicità e la sostenibilità delle aziende. Oggi in Italia esistono già aziende in diversi settori (ed esempio finanziario, energetico ed informatico) che vedono la cybersicurezza come una leva a supporto della strategia aziendale. Si tratta, tuttavia, di un fenomeno ancora a macchia di leopardo. La sfida consiste nel creare una massa critica di aziende, dalle grandi alle piccole e piccolissime, che siano in grade di governare la trasformazione digitale mitigando i rischi di cybersicurezza con un approccio proattivo che non si limiti alla gestione delle emergenze, ma preveda una strategia di resilienza a lungo termine, anche attraverso una collaborazione basata sulla fiducia tra aziende e istituzioni, *in primis* l'Acn.