ItaliaOggi Sette

diffusione:88589
tiratura:133263

Da un sondaggio Brunswick fra i componenti di Ccr: c'è gap tra consapevolezza e azione

La difesa contro i rischi cyber passa anche dalla governance

ROXY TOMASICCHIO

Bisogna passare velocemente dalle parole ai fatti, perché le minacce cyber alla sicurezza delle imprese stanno crescendo a ritmi vertiginosi e la domanda non è se un'azienda sarà colpita o meno da un hacker, ma quando questo succederà. La difesa? Passa da governance, comunicazione e formazione. La pensano così i consiglieri di amministrazione membri del Comitato controllo rischi (Ccr) coinvolti in un sondaggio svolto da Brunswick, società internazionale di consulenza, specializzata in comunicazione corporatefi nanziaria, tra i principali operatori nel campo della comunicazione in stato di crisi, che segue da tempo il tema del cyber crimine proprio per supportare le aziende nella protezione della reputazione. Dall'indagine, condotta in collaborazione con Nedcommunity (associazione dei consiglieri non esecutivi), e per cui è stato interpellato un campione di imprese pari al 48% della capitalizzazione dell'indice Ftse Mib (con le prime quattro in termini di valore, ossia Eni, Enel, Intesa Sanpaolo e Generali) e pari in assoluto al 37% della capitalizzazione delle società quotate su tutti i listini italiani, si rileva che c'è percezione molto forte che la protezione dal rischio cyber non è un tema solo tecnologico ma ancor prima è un tema di governance, di reputazione e di fl ussi di comunicazione e di formazione. Ma emerge anche una contraddizione tra questa percezione e le aspettative dei consiglieri di amministrazione e le azioni concrete da parte delle aziende. «Nonostante si registri un discreto livello di consapevolezza del rischio cyber, della sua importanza e priorità rispetto ad altri rischi aziendali, sia da parte dei membri dei comitati sia da parte dei cda, emerge come le politiche di governance messe in atto dai vertici aziendali per contenere il rischio aziendale siano ritenute poco effi caci e che quindi ci sia un gap da colmare fra la consapevolezza e l'azione», spiega a ItaliaOggi Sette Alessandro Iozzia, partner e direttore generale di Brunswick per l'Italia, che aggiunge come «lo stesso gap si registra sulla governance societaria, il ruolo della comunicazione e della preparazione di crisi attraverso l'assessment reputazionale e le esercitazioni di crisi». Infatti, tra i fattori ritenuti più importanti per la mitigazione del rischio di attacchi cyber emerge la formazione (punteggio di 3,88/4), seconda la protezione della security informatica (3,82/4) e subito dopo la protezione della reputazione insieme alla preparazione per affrontare la crisi (3,75/4). «Questi elementi vengono considerati, assieme alla sicurezza informatica e alla formazione delle persone, molto importanti per la mitigazione del rischio cyber», dice ancora Iozzia, «ma ancora una volta emerge come le aziende debbano, nella pratica, fare ancora molta strada per sviluppare attività mirate in tal senso. Il segnale che arriva da questo sondaggio è che occorre passare dalla teoria alla pratica, dalla consapevolezza all'azione e anche velocemente». In particolare, fra i rischi ritenuti più importanti per un'azienda dai membri dei Ccr spiccano ai primi tre posti: il rischio cyber in assoluto, il rischio reputazionale e quello fi nanziario. Di fronte a queste minacce, guardando ai risultati, Iozzia spiega che: «da una parte c'è una forte sensibilità da parte dei board members al tema cybersecurity (il 71% considera molto alto il rischio di un attacco cyber in confronto ad altri), alla necessità di fare formazione, di far esercitare il personale (il 76% pensa che sia molto importante svolgere un'esercitazione di tipo cyber per testare le procedure di risposta a un attacco cyber e verifi care i gap per migliorare i processi interni) e si dà importanza unanime alla comunicazione (l'88% dichiara molto alta l'importanza della comunicazione, il 12% abbastanza importante). Dall'altra parte però il riscontro concreto di

ItaliaOggi Sette

diffusione:88589
tiratura:133263

come le aziende rispondono al tema e di come i cda lo vivono è ancora incerto: solo il 23% dei consiglieri di amministrazione indipendenti valuta infatti come molto alta la consapevolezza da parte del cda delle conseguenze fi nanziarie, legali e di reputazione di un attacco cyber mentre il 53% lo reputa abbastanza alto e il 24% basso o molto basso. Il grado di effi cacia delle politiche di contenimento del rischio cyber è considerato molto alto solo dal 12% del campione mentre il 65% lo valuta abbastanza alto. Alla domanda se sia stato fatto un assessment del rischio reputazionale il 53% risponde di no, il 18% non è in grado di rispondere e solo il 29% risponde positivamente». All'opposto, l'assessment del rischio reputazionale in ambito cyber viene ritenuto molto importante da parte dei membri dei Ccr, al pari delle attività di comunicazione e di esercitazione di crisi in ambito cyber. Ma ancora una volta emerge come la strada verso la sicurezza sia ancora lunga.

L'importanza del rischio Cyber

Consapevolezza delle conseguenze di un incidente cyber

I rischi per un'azienda