Cyber risk ancora sottovalutato

PAGINA A CURA DI TANCREDI CERNE


ItaliaOggi7 IMPRESA Lunedì 13 Novembre 2017 15

Secondo l'indagine Aon-Ponemon Institute per asset materiali si spende quattro volte di più

Cyber risk ancora sottovalutato

Assicurato solo il 15% delle perdite massime stimate

Le principali ragioni di chi non si assicura contro il cyber risk

La copertura è inadeguata in base alla nostra esposizione
I costi delle polizze sono troppo alti
Sono sufficienti le nostre policy interne
Troppe esclusioni, restrizioni e rischi non assicurabili
Il management esecutivo non vede il valore di questa assicurazione
Impossibile ottenere assicurazione per il profilo di rischio attuale
L'assicurazione non copre certi rischi
Altro

Copertura offerta dalla compagnia di assicurazione

Sostituzione di apparecchiature perse o danneggiate
Perdita di produttività da parte dei dipendenti
Costi di notifica per le vittime di violazione dei dati
Spese per le comunicazione alle Autorità di regolamentazione
Responsabilità di terzi
Costi investigativi e legali
Multe e sanzioni comminate dalle Autorità di regolamentazione
Spese per la difesa legale
Perdite di produzione
Danni al brand
Altro
Non so

La spesa sostenuta dalle aziende europee per assicurarsi contro i rischi legati ad asset materiali è quattro volte superiore a quella per il cyber risk. E questo, nonostante il peso crescente dei costi derivanti dai furti di informazioni perpetrati dagli hacker sui server aziendali. «Nonostante la sempre maggiore consapevolezza dell' impatto del cyber crime, gli attacchi informatici continuano ad aumentare, con gravi conseguenze finanziarie per le imprese», ha avvertito Omar Abbosh, chief strategy officer di Accenture nel suo intervento a CyberTech Europe 2017 diffondendo i numeri relativi all' incidenza economica del cybercrime. «Il costo medio annuo per azienda sostenuto per gli attacchi informatici è cresciuto del 62% negli ultimi cinque anni. Le aziende devono iniziare a pensare alla sicurezza in modo diverso. A oggi, i cyber-attacchi stanno costando alle imprese del mondo una media di 11,7 milioni di dollari. Il primato per i danni più onerosi spetta agli Stati Uniti con 21,22 milioni di dollari, mentre in Italia il costo del cybercrime è di 6,73 milioni di dollari per azienda». Numeri di tutto rispetto che non sembrano, tuttavia, ancora sufficienti a convincere manager e imprenditori della rischiosità del fenomeno. E della necessità di assicurare la propria struttura contro questo genere di eventi. La conferma di tutto ciò è stata messa in luce dai risultati di un' inchiesta realizzata dal colosso assicurativo Aon in collaborazione con Ponemon Institute. «Nonostante le aziende riconoscano il crescente valore della tecnologia e dei dati rispetto agli asset materiali, continuano a spendere quattro volte in più per le coperture assicurative di rischi relativi a proprietà immobiliari, stabilimenti e attrezzature», hanno avvertito i curatori dello studio. Non solo. Secondo i risultati dell' inchiesta, il 38% delle aziende oggetto della ricerca avrebbe dichiarato di aver subito una perdita dovuta a un attacco cyber negli ultimi due anni per un valore medio di 3,3 milioni di dollari. Ma solo il 15% della perdita massima stimata per il cyber risk è risultata coperta da assicurazione. Risultato in contrasto con i massimali per

coprire i rischi di danni agli asset materiali (beni immobili, stabilimenti, attrezzature) per cui il 60% della perdita attesa è generalmente coperta. Il report ha mostrato inoltre come l' impatto dell' interruzione del business sul patrimonio di dati aziendale sia superiore del 50% rispetto a quello su proprietà immobiliari, stabilimenti e attrezzature. Fattore che da solo dovrebbe rappresentare una valida ragione per incrementare le coperture assicurative per questo genere di rischi. «La maggior parte delle aziende spende molto più in premi assicurativi contro incendi che in polizze contro attacchi cyber, nonostante dichiari nei documenti pubblici che una parte rilevante del valore aziendale sia attribuibile proprio agli asset intangibili», ha sottolineato Vanessa Leemans, chief operating officer di Aon per Global Cyber Insurance Solutions secondo cui il 65% circa delle aziende attive in Europa si aspetta che l' esposizione al rischio informatico aumenti nei prossimi due anni. «È molto importante che il cyber risk sia affrontato con un approccio integrato alla gestione dei rischi che coinvolga l' intera azienda per raggiungere un adeguato livello di resilienza contro gli attacchi informatici», ha aggiunto Leemans. «Questo richiede una formazione a tutti i livelli aziendali, sistemi di valutazione e quantificazione, una gestione del rischio a livello preventivo, piani di risposta agli incidenti, nonché adeguate coperture assicurative cyber». Ma come fare a convincere gli imprenditori a muoversi nella giusta direzione evitando di trascurare rischi importanti? «Per le aziende la gestione dei rischi cyber è più complessa di quella dei rischi tradizionali e va affrontata a tutto tondo», ha avvertito Enrico Vanin, numero uno di Aon SpA e Aon Hewitt Risk&Consulting. «Il primo passo da compiere è quello di creare consapevolezza da parte del top management e delle funzioni operative riguardo alle minacce cyber e all' impatto sul business. Successivamente è necessario sviluppare processi integrati di risk management che prevedano meccanismi di prevenzione, controllo, real time monitoring, incident response e insurance transfer». La sfida del regolamento privacy. Soltanto il 30% delle aziende è pienamente consapevole delle conseguenze legali ed economiche legate all' entrata in vigore del Regolamento generale sulla protezione dei dati (Gdpr) dell' Unione europea prevista per il mese di maggio del prossimo anno. E ancora pochi stanno spingendo sull' acceleratore per arrivare preparati all' appuntamento. Secondo un sondaggio condotto da Isaca tra dirigenti senior e membri dei consigli di amministrazione, infatti, meno di un terzo degli intervistati si è detto soddisfatto dei progressi raggiunti dalle rispettive aziende riguardo alla preparazione per il Regolamento. Mentre un preoccupante 35% non è nemmeno a conoscenza dei progressi compiuti dall' azienda. La normativa comunitaria prevede che gli utenti debbano dare autorizzazioni più specifiche alle aziende e potranno revocarle se non saranno più d' accordo; inoltre, potranno richiedere informazioni su come vengono gestiti i propri dati, dove e per quale scopo. Non solo. Ogni utente potrà richiedere alle aziende le informazioni che utilizzano su di lui e ottenerne la cancellazione dai server dell' azienda stessa. Infine, le aziende dovranno studiare come gestire la protezione dei dati fin dalla progettazione di nuovi sistemi, in modo da seguire il principio di «privacy by design». E le società la cui attività prevede la manipolazione di un volume importante di dati personali, dovranno disporre di un responsabile che si occupi della loro protezione. Queste misure hanno l' intento di

ridurre la probabilità di fughe di dati; tuttavia, se ciò dovesse accadere, le aziende avranno l' obbligo d' informare le autorità competenti entro 72 ore fatta eccezione per quelle che non rappresentano un rischio per i singoli. In caso di inadempienza al Regolamento, le sanzioni potranno arrivare fino a 20 milioni di euro o al 4% del fatturato globale (a seconda di quale sia l' importo maggiore). © Riproduzione riservata.