PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4784 di Mercoledì 30 settembre 2020

Forse è bene riesaminare le polizze sui rischi informatici

Molte aziende ormai da tempo hanno attivato delle polizze sui rischi informatici, chiamate con termine "cyberinsurance". L'evoluzione del mercato riflette l'evoluzione dei rischi e forse è opportuna una rivalutazione attenta delle coperture in essere.

Il responsabile dei sistemi informatici aziendali sa benissimo che l'ipotesi che non si verifichi mai alcun rischio, afferente al sistema informatico, è priva di fondamento. Il responsabile può adottare tutti i possibili ragionevoli applicativi di sicurezza del sistema informatico, ma il rischio che possa verificarsi qualche guaio è sempre immanente.

Questa è la ragione per cui ormai quasi tutte le aziende, non solo di media e grande dimensione, hanno deciso di dotarsi di una polizza contro i rischi informatici. Queste polizze, per la gran parte, si appoggiano a sottoscrittori specializzati dei Lloyd's, che fin dal 1980 avevano presentato sul mercato questo tipo di copertura.

Come è evidente, il premio per queste polizze rispecchia non solo i rischi che vengono presi in considerazione, ma anche la storia di questi rischi. Negli ultimi tempi, anche grazie alla crescente diffusione di alcuni principi fondamentali di responsabilità, enunciati dal regolamento generale europeo sulla protezione dei dati personali, ed in particolare le responsabilità afferenti a data breach, sia di ordine colposo, sia di ordine doloso, le sanzioni applicate sono cresciute notevolmente.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0551] ?#>

I sottoscrittori dei Lloyd's, negli ultimi due anni, sono stati subissati da richieste di risarcimenti per perdite, dovute a violazioni dei dati, che hanno portato come conseguenza due tipi di danni:

- il danno afferente all'applicazione di una sanzione amministrativa pecuniaria, da parte dell'autorità nazionale coinvolta,
- il danno afferente al risarcimento dovuto agli interessati, a seguito di possibili conseguenze negative, direttamente riconducibili alla violazione dei dati.

Il mercato è cresciuto, ma sono anche cresciuti i rischi ed ecco il motivo per cui è opportuno effettuare una valutazione aggiornata dei rischi aziendali, per poter determinare le coperture appropriate. Tanto per dare un'idea delle dimensioni del mercato, il mercato per queste coperture, nei soli Stati Uniti, presenta un ammontare dei premi variabile fra i 2,5- 3, 5 miliardi di dollari e gli esperti prevedono che nei prossimi tre anni il mercato potrebbe aumentare del 40%.

Durante una recente indagine, il 47% degli intervistati ha dichiarato di aver attivato una polizza assicurativa per i rischi informatici, rispetto al 34% nel 2017. Le risposte di molti intervistati hanno però messo in evidenza come non tutti abbiano un'idea chiara su quali siano gli scenari di rischio coperti dalle polizze assicurative, e quali siano i limiti applicabili ai risarcimenti. Un altro aspetto, spesso sottovalutato, riguarda un attento esame dell'evoluzione del rischio, nei prossimi sei mesi o anni, in modo da mantenere sempre allineata la copertura con i rischi.

Ad esempio, la migrazione verso il cloud di molti trattamenti informatici, precedentemente svolti in azienda, cambia in modo significativo lo scenario di rischio ed occorre effettuare una attenta valutazione comparata delle coperture aziendali, rispetto alle coperture del gestore del cloud. Un altro aspetto, spesso sottovalutato, riguarda il danno d'immagine all'azienda. Se si verifica una violazione di dati nel cloud, gestito da un fornitore terzo, è l'immagine dell'azienda che viene coinvolta, assai più dell'immagine del fornitore terzo.

Inoltre, spesso la copertura assicurativa viene valutata solo da un ramo dell'azienda coinvolta, mentre essa dovrebbe essere valutata, come minimo, da un rappresentante dell'alta direzione, da un rappresentante legale e dal responsabile del sistema informativo. Il fatto di appoggiarsi ad un broker, invece che direttamente ad una compagnia di assicurazione, in certi casi può offrire un valore aggiunto, legato alla competenza specifica nel settore del broker prescelto.

Chi scrive per anni ha svolto attività di security Surveyor su queste tipologie di polizze, in appoggio ai maggiori sottoscrittori londinesi, e ricorda ancor oggi il messaggio che veniva lanciato da questi sottoscrittori: "Quando si valutano i parametri di una polizza informatica, occorre scegliere il più alto massimale, che può essere accettato dal sottoscrittore, nonché il più alto scoperto, o franchigia, che può essere sopportato dall'assicurato".

Basta dare un'occhiata alle sanzioni recentemente applicate dalle maggiori autorità Garanti nazionali, in relazione a vari tipi di violazione del regolamento europeo, per rendersi conto che importi milionari, in euro, non sono affatto insoliti, ma anzi stanno diventando spesso quasi una norma.

È ben vero che il regolamento europeo afferma che la sanzione pecuniaria amministrativa deve essere "effettiva, proporzionata e dissuasiva". Ciò significa che, a parità di tipologia di violazione, l'importo della sanzione amministrativa applicata ad una grande azienda è enormemente superiore, rispetto all'importo applicato ad una piccola azienda, proprio perché il valore dissuasivo per una grande azienda può essere valutato a milioni di euro, mentre per una piccola azienda può essere valutato a qualche decina di migliaia di euro.

Infine, mi permetto di richiamare l'attenzione dei lettori anche su alcuni aspetti connessi alla copertura assicurativa, vale a dire la copertura dei costi legali e delle attività dei consulenti informatici, che spesso vengono coinvolti. Questi consulenti informatici possono presentare parcelle estremamente elevate ed ecco la ragione per la quale una appropriata copertura assicurativa contro i rischi informatici deve comprendere anche i rischi legali, nonché i rischi connessi alle attività dei consulenti tecnici coinvolti.

A questo punto, mi auguro che i lettori prendano in mano le polizze esistenti e comincino a riesaminarle con molta attenzione, guardando non solo al domani, ma anche al dopodomani!

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it