ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4705 di Lunedì 25 maggio 2020

L'assicurazione sul Computer Crime in tempi di COVID 19

Le principali aziende assicurano i propri sistemi informativi contro i rischi di criminalità informatica ed eventi accidentali. Questa assicurazione ha bisogno di essere rivalutata davanti a scenari assai preoccupanti, come una pandemia.

Chi scrive si occupa di valutazione del rischio legato a crimini informatici ormai da decenni ed ha perfino scritto un volume sull'argomento, nel 1993. Gli scenari di rischio informatico sono in continua evoluzione e di conseguenza devono anche aggiornarsi le coperture contro questi rischi. Le numerose notizie, che appaiono sui mezzi di comunicazione di massa, afferenti a tentativi di attacco informatico, soprattutto tramite posta elettronica, che sono aumentati in modo esponenziale degli ultimi mesi, suggeriscono ai responsabili della continuità operativa informatica dell'azienda di effettuare una valutazione critica ed aggiornata delle coperture assicurative contro questi rischi.

Vediamo di fare il punto della situazione.

Tanto per cominciare, occorre separare in maniera univoca il rischio legato a danneggiamenti che coinvolgono gli apparati informatici, che sono coperti dalla cosiddetta polizza elettronica, dai rischi che invece coinvolgono il funzionamento degli apparati stessi, l'archivio dei dati, gli applicativi e le funzionalità operative.

Questo tipo di copertura assicurativa era classificato, dai sottoscrittori dei Lloyd's di Londra, con l'acronimo CCC-Computer Crime Coverage. È una copertura oltremodo complessa, che richiede sempre il sopralluogo da parte di un esperto accreditato dai sottoscrittori, che effettua una valutazione oggettiva dello scenario di rischio e offre indicazioni sulle misure di messa sotto controllo. Questa valutazione di rischio può essere condotta su incarico del broker assicurativo, oppure del sottoscrittore dei Lloyd's, cui la richiesta di copertura verrà successivamente presentata.

La rapida nascita di nuove tecnologie, come ad esempio bitcoin, blockchain e simili, richiede un costante aggiornamento delle coperture, a livello di tipo di rischio coperto, di massimali e di eventuali franchigie.

Proviamo ad analizzare insieme i punti qualificanti di una copertura informatica.

? Molti assicuratori dispongono di propri schemi di misure protettive, cui l'assicurato deve adeguarsi. Occorre verificare se e come il sistema informativo dell'assicurato è allineato con queste misure protettive minime, imposte dall'assicuratore.

? È indispensabile effettuare un'analisi attenta di tutte le esclusioni presenti in una copertura assicurativa informatica, per essere certi che tutti i rischi prevedibili siano ragionevolmente coperti. Non stiamo parlando evidentemente di rischi legati alla

trasmutazione dell'atomo, a fulminazioni od altro, ma stiamo parlando di scenari, come ad esempio quello legato alla perdita di una chiavetta di memoria, sulla quale siano archiviati dati non protetti da algoritmo crittografico. Nella stragrande maggioranza delle coperture assicurative, di questo scenario di rischio non si prevede copertura.

? Oggi sempre più diffuse sono le tecniche di protezione crittografica, che sono per solito di alto livello, ma spesso presentano un punto debole nelle modalità di gestione delle chiavi di codifica e decodifica. Una aggiornata ed efficace protezione delle chiavi spesso è ancora più importante, rispetto all'adozione di protocolli crittografici di altissimo livello, come ad esempio AES-Advanced Encryption Standard o algoritmi similari.

? Il fatto che i rischi evolvano rapidamente impone che il piano di valutazione del rischio del sistema informativo dell'azienda sia aggiornato con pari rapidità. Una analisi di rischio che non viene aggiornata per molti mesi con ogni probabilità non rispecchia più né il sistema informativo aziendale coinvolto, né i rischi che tale sistema deve fronteggiare.

? Spesso le coperture assicurative utilizzano espressioni che sono comprensibili per chi lavora nel settore, ma potrebbero non essere altrettanto comprensibili per i responsabili della sicurezza informatica. In questi casi l'appoggiarsi ad un broker, che vive in questo mondo, può rappresentare un prezioso appoggio per chiarire i principali aspetti della copertura assicurativa. Ad esempio, il fatto di archiviare dati nel cloud presenta evidentemente dei rischi, che la copertura assicurativa deve correttamente inquadrare e coprire. Non sempre i termini di questa specifica estensione della copertura sono sufficientemente intelligibili per un "normale" chief security officer.

? Poiché il mercato è abbastanza attraente, su di esso possono apparire degli assicuratori, che non hanno una sufficiente esperienza e tradizione. Questo è motivo per cui è indispensabile che l'assicurato si accerti del livello di affidabilità e competenza della compagnia, cui intende affidarsi. Anche in questo caso, l'utilizzo di un broker può esser oltremodo utile per offrire adeguate garanzie, consolidate nel tempo.

? Il regolamento generale sulla protezione dei dati ha introdotto livelli di sanzioni, in caso di violazione dei dati, che potrebbero essere estremamente elevati. Ricordo che nessuna copertura assicurativa copre le sanzioni di natura penale, mentre è possibile ottenere copertura per le sanzioni di natura amministrativa. Poiché l'assicuratore deve essere oltremodo prudente su questi aspetti, non deve stupire l'assicurato il fatto che vengano posti franchigie, coperti e massimali relativamente contenuti.

? Occorre fare attenzione alla differenza fondamentale che esiste fra la copertura dei danni diretti e quella relativa ai danni indiretti. Ad esempio, la copertura per danni diretti può coprire le spese di ricostruzione di un data base danneggiato, mentre non è detto che possa coprire i danni relativi al fatto che, durante il periodo di ricostruzione dei dati, i servizi informatici che vengono resi dall'azienda danneggiata non siano possibili o siano possibili solo con forti limitazioni.

? In caso di violazione dei dati, la compagnia assicuratrice può dare copertura per i rischi legali, ma solo a condizione di appoggiarsi a studi legali affidabili e competenti. È una situazione simile a quella che può trovare chi assicura la propria autovettura per danni: la compagnia di assicurazione può coprire questi danni, solo se ci si rivolge a carrozzieri o a meccanici autorizzati.

In sintesi, la copertura assicurativa per questi rischi è decisamente articolata e, ad oggi, non esiste una copertura standardizzata, come invece esisteva nel lontano 1980, cioè già menzionata polizza assicurativa CCC.

Oggi i rischi sono sempre più elevati, gli scenari sono sempre più complessi e un costante aggiornamento delle condizioni di polizza, supportate da un esperto specializzato, rappresenta una necessità, più che un'opportunità.

Adalberto Biasiotti