PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4595 di Mercoledì 04 dicembre 2019

L'evoluzione delle polizze sui rischi informatici

I principali assicuratori mondiali hanno recentemente introdotto nuove coperture sui rischi informatici, a fronte di uno scenario in costante evoluzione. Ecco una breve sintesi dell'evoluzione delle coperture assicurative su questi rischi specifici.

Nata più di un secolo fa, la copertura assicurativa offerta dai Lloyd's al mondo dell'istituzione finanziaria venne chiamata BBB, come acronimo di Bankers Blanket bond, vale a dire garanzia ad ombrello per il mondo bancario.

Sulla base di questo acronimo, venne successivamente messa a punto, intorno alla fine degli anni 70, una polizza informatica, che venne chiamata CCC, acronimo di Computer Crime Coverage.

Chi scrive operò come security Surveyor, nell'interesse di un sottoscrittore dei Lloyd's, per accendere in Italia la prima polizza di questo tipo, richiesta da un grande centro di elaborazione dati, al servizio del mondo bancario.

Successivamente questa polizza si è estesa rapidamente non solo al mondo bancario, ma anche al mondo dell'industria, che si stava rendendo conto del fatto che i rischi afferenti al sistema informativo potevano essere ben maggiori, rispetto ai rischi afferenti a furti o rapine, che potevano coinvolgere il patrimonio mobiliare.

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

Con il passare del tempo questa copertura assicurativa si è costantemente voluta, ma l'evoluzione degli scenari di attacco è stata decisamente più rapida ed ecco la ragione per la quale oggi stanno nascendo nuove coperture, in grado di aiutare l'assicurato a fronteggiare nuove tipologie di rischi.

Queste coperture oggi sono disponibili non solo per le istituzioni finanziarie, ma anche per le aziende, manifatturiere e non, ed i liberi professionisti, che possono anch'essi essere soggetti a rischi di questo tipo.

Questa nuova copertura viene spesso chiamata con l'acronimo CLI -cyber liability insurance, che esplicitamente prende in carico rischi, che nemmeno venivano sognati solo 10 anni fa.

In genere queste coperture devono essere personalizzate ed offrono all'assicurato tutta una serie di rischi, per i quali egli può chiedere protezione.

Ecco un esempio delle coperture disponibili:

- distruzione fisica di supporti informatici,
- furto o copia abusiva di supporti informatici,
- copertura di danni legati ad estorsione, conseguente ad un attacco ransomware,
- copertura dei danni all'hardware conseguenti ad incendi o allagamenti od eventi sismici,
- copertura dei costi in cui si incorre, quando si devono informare i clienti circa una violazione della sicurezza, che può avere riflessi diretti sui clienti stessi; ad esempio allestimento di un numero verde,
- copertura delle spese legali, conseguenti a rivendicazioni di terzi danneggiati o alla gestione di contestazioni, nei confronti di sanzioni emesse dalle autorità Garanti della protezione dei dati,
- copertura dei costi necessari per consentire a specialisti del settore di recuperare dati su supporti danneggiati,
- copertura dei costi necessari per ricostruire ex novo dati non recuperabili.

Lo studio di queste coperture e l'adattamento delle coperture disponibili alle esigenze dello specifico assicurato richiede uno studio approfondito e richiede, innanzitutto, la conduzione di un'analisi di rischio, effettuata da uno specialista, gradito sia all'assicurato, sia all'assicuratore.

Si raccomanda caldamente che l'analisi di rischio, effettuata dal security Surveyor informatico, venga condotta in conformità a una vigente norma europea, in modo da dare ogni possibile garanzia che tale analisi sia condotta in conformità allo stato dell'arte.

Il fatto di utilizzare una norma europea fa sì che la valutazione di rischio sia valida in tutta Europa e venga così accolta da assicuratori e riassicurator,i ovunque essi si trovino.

Un altro aspetto essenziale riguarda la scrittura della valutazione di rischio in lingua inglese, in quanto, anche se l'assicuratore ha sede in Italia, nella stragrande maggioranza dei casi egli si riassicura presso compagnie di riassicurazione specializzate, tra cui in prima fila sono evidentemente i sottoscrittori ai Lloyd's.

L'analisi di rischio deve essere personalizzata, in quanto devono essere presi in considerazione solo i rischi, per i quali l'assicurato desidera trovare copertura, e questo fatto influenza in modo significativo la parcella dell'esperto. Nell'esperienza di chi scrive, la parcella è spesso pagata dall'assicurato, ma, in qualche caso, in cui l'assicurato riveste un ruolo particolarmente prestigioso, può essere perfino l'assicuratore che si accolla il costo relativo.

Un altro aspetto essenziale riguarda il fatto che l'analisi di rischio deve essere periodicamente aggiornata, proprio per rispecchiare in modo puntuale l'evoluzione degli scenari di attacco.

Per quanto riguarda i massimali e le franchigie da inserire in polizza, mi permetto di ricordare un consiglio che mi dette anni fa uno dei maggiori sottoscrittori dei Lloyd's, specializzato proprio in polizze informatiche: "l'assicurato deve chiedere il più elevato massimale possibile, indicando al contempo la più elevata franchigia, che egli si sente di accollarsi".

È un consiglio che sono lieto di condividere con i lettori, in quanto ritengo sia perfettamente valido ancora oggi!

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it