PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5009 di Lunedì 20 settembre 2021

È una buona idea assicurarsi contro i ricatti da ransomware?

Il crescente numero di attacchi per ransomware ha indotto molte aziende ad estendere la propria copertura assicurativa anche a questo tipo di attacco. Tuttavia i pareri degli esperti su questo approccio sono assai diversi.

L'aumento della frequenza degli attacchi per ransomware ha indotto molte aziende ad attivare, oppure ad estendere, coperture assicurative contro questo ricatto. Tuttavia, uno studio recentemente sviluppato nel Regno Unito ha messo in evidenza come questa situazione potrebbe tornare a favore degli attaccanti, che potrebbero aumentare il numero degli attacchi ed aumentare la richiesta di riscatto, confidando sul fatto che il soggetto attaccato sia coperto dall'assicurazione. Ci si domanda poi se sia legittimo, in linea di principio, trovare una copertura contro un atto delittuoso di questo tipo.

Ricordo ai lettori che in Italia è proibito offrire coperture assicurative per la richiesta di riscatto, a seguito del rapimento di una persona. Per contro, ai Lloyd's queste coperture sono correntemente utilizzate, ad esempio per proteggere i dirigenti aziendali che vanno ad operare in zone ad alto rischio di rapimento, come ad esempio Sudamerica.

Indipendentemente quindi dalla legittimità o meno di ottenere tali coperture, le perplessità, illustrate in uno specifico documento di un ente di ricerca, dal titolo

"Cyber Insurance and the Cyber Security Challenge" di Jamie MacColl, Jason R C Nurse and James Sullivan del Royal United Services Institute for Defence and Security Studies

sono significative.

Uno dei primi problemi messi in evidenza sta nel fatto che molte aziende possono pensare di proteggersi da questi attacchi con la copertura assicurativa, invece di attivare ben più efficienti, efficaci e significative protezioni del proprio sistema informatico.

D'altro canto, l'esperienza mostra che, mano a mano che gli assicuratori si trovano a dover rimborsare significativi sinistri, essi emanano degli standard di sicurezza ancora più restrittivi, rispetto a quelli che possono essere indicati dalle strutture nazionali di sicurezza informatica, a pena di non ottenere una copertura assicurativa.

Ancora oggi, i lettori sanno benissimo che, in assenza di disposizioni nazionali in merito a misure minime di sicurezza per alcune attività commerciali, sono gli assicuratori che stabiliscono degli standard minimi, al di sotto dei quali essi non sono disposti a dare copertura. Ciò vale, ad esempio perfino per le abitazioni private. Molte compagnie assicurative non danno protezione assicurativa, se non è installata una porta d'ingresso anti effrazione di soddisfacenti caratteristiche e le vie di accesso non sono protette in modo altrettanto efficace.

D'altro canto, appare evidente come l'obiettivo di una copertura assicurativa per i rischi informatici non è quella di fungere da strumento alternativo all'adozione di efficienti ed efficaci misure di protezione, ma solo di offrire copertura contro il rischio residuo, che può comunque sussistere, anche se l'assicurato ha adottato avanzati sistemi di sicurezza.

Il documento messo a punto dai ricercatori, menzionati in precedenza, prende in esame tutti gli aspetti positivi e negativi della copertura assicurativa, in modo da consentire ai responsabili aziendali di assumere decisioni tali da trovare un corretto equilibrio fra l'investimento necessario per elevare il livello di sicurezza del sistema informativo e il costo di un premio assicurativo.

Al proposito, mi permetto di ricordare che mentre gli investimenti nell'aumentare il livello di sicurezza del sistema informativo vanno in conto capitale e quindi non influenzano negativamente il bilancio aziendale, i costi afferenti ad un premio assicurativo vanno nelle voci di uscita corrente, costituendo quindi un aumento non ammortizzabile dei costi.

Inoltre, non dimentichiamo che, per quanto una copertura assicurativa sia completa, vi sono sempre delle riserve, messe debitamente in evidenza nel testo di polizza, che potrebbero far sì che, in determinate circostanze, la copertura assicurativa non sia valida oppure lo sia con forti limitazioni.

Occorre inoltre tener presente che il mercato assicurativo, per queste particolari coperture, è in continua evoluzione, soprattutto perché ad oggi la disponibilità di dati oggettivi su questo tipo di sinistri non è tale da consentire alle compagnie assicurative di effettuare proiezioni credibili. Ciò impedisce agli assicuratori di quantificare in modo corretto sia le cause sia gli effetti dei sinistri e ciò comporta l'assunzione di atteggiamenti estremamente prudenziali. La presenza di incidenti drammatici, come quello che ha colpito la rete di trasmissione energetica della costa orientale degli Stati Uniti, ha limitato la disponibilità degli assicuratori ad assumere questi rischi.

Una possibile soluzione a questo problema si può trovare inserendo in polizza l'obbligo tassativo di non diffondere in alcun modo la presenza di questo tipo di copertura, per evitare che i malviventi possano chiedere riscatti più elevati e possano scegliere aziende, che più facilmente potranno accedere alla richiesta estorsiva.

Il documento si conclude offrendo una serie di possibili misure di intervento, come ad esempio la indicazione di minimi livelli di sicurezza informatica da rispettare, prima di poter cercare una copertura assicurativa, oppure un miglioramento della rete di raccolta e diffusione dei dati afferenti a sinistri, nonché la creazione di un nuovo approccio collaborativo fra gli assicurati, gli

assicuratori e le forze dell'ordine.

Ancora una volta, il documento si chiude ricordando che l'obiettivo primario di una copertura assicurativa non è quella di migliorare il livello di sicurezza dagli attacchi informatici, ma quello di assorbire l'eventuale rischio residuo.

Adalberto Biasiotti

www.puntosicuro.it