

Assicurazioni contro gli attacchi informatici: cosa dovrebbero coprire e quanto convergono davvero?



Fortune Business Insights ha valutato il mercato delle assicurazioni informatiche in oltre 10 miliardi di dollari nel 2021 e prevede una crescita di oltre 63 miliardi di dollari entro il 2029. Con la crescente diffusione delle minacce informatiche e gli elevati costi associati alla risposta e al recovery dopo un incidente informatico, molte aziende e privati stanno valutando l'acquisto di un'assicurazione informatica per mitigare i rischi.

Rispetto alle prime forme diffuse negli anni Novanta che coprivano una serie piuttosto ristretta di eventi, le attuali polizze assicurative contro i rischi informatici hanno a oggetto un'ampia gamma di conseguenze digitali e reali degli attacchi informatici. La valutazione di ciò che costituisce una buona polizza informatica varia, quindi, in modo significativo in base al settore in cui opera l'organizzazione. Ecco alcuni punti di partenza per comprenderne le possibilità.

Violazione dei dati

Una violazione dei dati si verifica quando persone non autorizzate hanno accesso o riescono a impossessarsi di informazioni sensibili, come i dati dei clienti o le informazioni aziendali proprietarie. Una polizza assicurativa contro le minacce informatiche dovrebbe coprire i costi associati alla risposta a una violazione dei dati, come l'assunzione di un investigatore forense, la notifica alle

persone colpite e l'offerta di servizi di monitoraggio del credito. È possibile negoziare clausole aggiuntive per coprire le multe e le sanzioni previste dalla normativa in determinate situazioni.

Interruzione dell'attività

Un attacco informatico o una violazione dei dati possono interrompere le attività di un'azienda, con conseguente perdita di entrate e aumento delle spese. Una buona polizza assicurativa contro le minacce informatiche dovrebbe coprire i costi associati all'interruzione dell'attività, compresi i mancati guadagni e le spese aggiuntive sostenute a causa dell'incidente. Alcune polizze coprono ulteriori spese di continuità aziendale, come la sostituzione di apparecchiature danneggiate o il mancato adempimento di obblighi contrattuali a causa di attacchi informatici.

Attacchi ransomware

Il ransomware è un tipo di software malevolo che cripta i dati della vittima e le chiede un riscatto alla vittima per ripristinare l'accesso agli stessi. Una polizza di assicurazione informatica dovrebbe coprire i costi associati alla risposta a un attacco ransomware, compresi il pagamento del riscatto (se necessario) e l'assunzione di una società di cybersecurity per ripristinare i sistemi colpiti. È importante ricordare che ci sono stati casi in cui l'assicuratore ha pagato il riscatto, ma gli aggressori non hanno ripristinato l'accesso ai dati.

Responsabilità civile

Una polizza di assicurazione cyber dovrebbe anche fornire una copertura di responsabilità civile nel caso in cui un'azienda venga citata in giudizio per non aver protetto adeguatamente i dati dei propri clienti o dei dipendenti.

Oltre alle caratteristiche generali di cui sopra, è bene essere attenti anche ad alcune “sfumature” precedenti e successive all’incidente di sicurezza. Tra queste:

Copertura della tecnologia aziendale o operativa

La maggior parte dei team di Procurement riceve l’indicazione di “stipulare la polizza il prima possibile al miglior prezzo” e quindi procede a ottenere la copertura per i sistemi aziendali standard e non per quelli OT. Ciò può far sì che un incidente significativo avvenuto in un ambiente OT resti scoperto.

Copertura dei costi operativi al di là del lavoro iniziale di risposta agli incidenti

A volte il processo di bonifica richiede una spesa di un ordine di grandezza superiore al budget delle operazioni IT. Inoltre, se vengono coinvolte le Forze dell’ordine, spesso i costi operativi possono protrarsi per anni, a causa delle regole in materia di cooperazione (o per ritardare la divulgazione, sottoponendo così l’azienda a ulteriori rischi).

Danni a terzi

È bene assicurarsi che la polizza assicurativa contro le minacce informatiche preveda una copertura sufficiente per i danni causati a terze parti. Ad esempio, nel caso in cui gli account della vittima iniziale vengano utilizzati per accedere ai sistemi di un fornitore terzo. Le richieste di risarcimento del fornitore sono spesso limitate dalle clausole, con costi significativi a carico dell’azienda.

Danni fisici

Con la gestione degli edifici e i sistemi meccanici controllati tramite applicazioni, è possibile creare condizioni ambientali all'interno del datacenter o altrove che possono causare danni fisici alle risorse. È importante assicurarsi che i piani di disaster recovery siano testati per garantire che le richieste di risarcimento della polizza non siano ostacolate.

Come possono, quindi, le aziende valutare le proprie esigenze di assicurazione informatica? Ci sono alcuni fattori chiave da considerare per determinare l'entità della copertura assicurativa necessaria:

- **le dimensioni e la complessità dell'azienda.** Le aziende più grandi, con sistemi più complessi e un volume maggiore di dati sensibili, possono richiedere una copertura più completa. Questa dovrebbe includere ipotesi di fusione e acquisizione per assicurarsi che la polizza copra l'azienda nel caso in cui questa cambi materialmente dimensioni e portata. È necessario uno stretto coordinamento tra i leader esecutivi, in particolare il CFO e il CISO, in quanto entrambi si occupano di mitigare rischi simili, ma guardando attraverso lenti uniche e talvolta non coordinate.
- **il settore in cui opera l'azienda.** Alcuni settori, come quello sanitario e finanziario, possono essere a maggior rischio di attacchi informatici e richiedere una copertura più robusta.
- **la capacità dell'azienda di assorbire i costi di un incidente informatico.** Le aziende con risorse limitate potrebbero non essere in grado di sostenere i costi associati a un attacco informatico o a una violazione dei dati senza una copertura assicurativa.
- **il controllo sulla riservatezza dell'incidente.** Alcune organizzazioni scelgono di stipulare contratti di

risposta agli incidenti in modo indiretto con società terze, attraverso strumenti legali. È importante valutare se la polizza assicurativa lo consente e comprendere gli accordi di riservatezza in essere tra l'azienda e le parti coinvolte.

Resta da chiedersi se l'assicurazione contro le minacce informatiche valga la pena di essere stipulata nel lungo periodo. La risposta è che dipende dalle esigenze e dalle circostanze specifiche dell'azienda o del singolo. Per le aziende, i costi di risposta a un incidente informatico possono essere significativi e, in alcuni casi, una polizza di assicurazione informatica può fornire la protezione finanziaria necessaria. Per i privati, la decisione di acquistare un'assicurazione informatica può dipendere dalla quantità e dalla sensibilità dei dati personali che si trovano online e dalla disponibilità a sostenere i costi di un potenziale attacco informatico. In definitiva, è importante che le aziende e i privati considerino attentamente le proprie esigenze di assicurazione informatica e soppesino i potenziali costi e i benefici di una copertura.

È importante coinvolgere l'assicuratore in tutte le fasi di un incidente, dalle esercitazioni a tavolino che includono la comunicazione con l'assicuratore in un incidente simulato, fino alle prime fasi dell'indagine. Una comunicazione chiara e frequente con l'assicuratore rende molto più facile la presentazione della richiesta di risarcimento finale.

In generale, c'è molto da imparare quando si intraprende la strada dell'assicurazione informatica. Se vi rivolgete a un fornitore per tempo, questi vi consiglierà fornitori di servizi di risposta agli incidenti di terze parti con cui ha negoziato le tariffe e che hanno ottenuto risultati positivi per i propri clienti. Il viaggio è la destinazione, e nel caso degli incidenti informatici questo è molto vero.

A cura di **Brian Neuhaus**, *CTO Americas*, e **Aaron Turner**, *CTO*

SaaS di Vectra AI

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/assicurazioni-contro-gli-attacchi-informatici-cosa-dovrebbero-coprire-e-quanto-convergono-davvero/>