SE NON ORA, QUANDO? L'IMPORTANZA DI ESSERE PRONTI PER IL RISCHIO INFORMATICO

La crescente prospettiva di un attacco informatico è una delle principali minacce all'attenzione dei professionisti del rischio di tutto il mondo. La frequenza degli incidenti e le loro possibili conseguenze sono motivo di preoccupazione per le aziende di tutte le dimensioni e di tutti i settori

di Luca Ricca, Head of Financial Lines, Insurance, Italy da SOMPO *www.sompo-intl.com*

I cyberattacchi sono una minaccia importante per l'Italia, che nel 2022 si posizionerà al quarto posto nel mondo e al primo in Europa per numero di cyberattacchi, secondo la US International Trade Administration[1] . Il costo medio di un incidente di violazione dei dati in Italia ha raggiunto i 4,73 milioni di dollari nel 2024, mentre il costo totale della criminalità informatica in Italia ha superato i 66 miliardi di dollari nel 2023 (Statista[2]).

La minaccia informatica si sta evolvendo. Gli hacker non sono più solo attori solitari ma, sempre più spesso, fanno parte di reti criminali altamente organizzate e dotate di buone risorse. Non solo i loro attacchi sono più mirati, ma i criminali informatici di oggi impiegano nuove tecniche e tattiche, come l'utilizzo dell'intelligenza artificiale (AI) per creare video falsi con cui estorcere riscatti.

La consapevolezza del rischio informatico è elevata tra le aziende e gli intermediari in Italia. La Banca d'Italia, il Ministero dell'Economia e delle Finanze e l'Agenzia Nazionale per la Cybersecurity sono tra le parti che collaborano per migliorare la prevenzione del rischio informatico[3] . Le organizzazioni dispongono di solide procedure e controlli. Queste includono l'aggiunta di patch, la scansione continua e l'applicazione di aggiornamenti di sicurezza; l'assicurazione che l'autenticazione a più fattori (MFA) sia in funzione; l'uso di software EDR (endpoint detection response) per proteggere le postazioni di lavoro e i server; e l'assicurazione che i sistemi siano sottoposti a backup offline, oltre ad altre misure.

Nel caso del cyber, la tua forza è pari a quella del tuo anello più debole. Troppo spesso le fragilità sono all'interno dell'organizzazione stessa. È importante che tutti all'interno dell'azienda, dal più giovane al più anziano, siano consapevoli dei rischi informatici e di come reagire ad essi. E questa formazione deve essere sempre aggiornata per garantire che tutti sappiano cosa fare in caso di incidente informatico.

I risk manager sono anche consapevoli del fatto che non bisogna considerare solo il rischio diretto per la propria organizzazione. In un mondo sempre più interconnesso, le aziende possono essere colpite da violazioni di fornitori e venditori che possono essere collegati ai loro sistemi e avere accesso a dati critici, ad esempio.

È quindi fondamentale che le aziende si assicurino di avere una supervisione dei sistemi di sicurezza delle terze parti con cui lavorano e di confidare nella solidità dei protocolli di gestione del rischio e della protezione da esse attuati.

[1] https://www.trade.gov/country-commercial-guides/italy-cybersecurity
[2] https://www.statista.com/topics/12128/cyber-crime-and-companies-in-italy/#topicOverview
[3] https://www.bancaditalia.it/focus/cybersicurezza/educazione-cyber/index.html?com

> *È importante che tutti all'interno dell'azienda, dal più giovane al più anziano, siano sempre consapevoli dei rischi informatici e di come reagire ad essi*

Ma anche con i migliori protocolli di sicurezza, non è mai possibile essere protetti al 100% da un attacco informatico. È una questione di quando, non di se, un attacco avrà luogo. I risk manager sanno che per ridurre al minimo i danni causati alle attività della loro azienda da un attacco, hanno bisogno di un piano per gestire un incidente e per riportare i sistemi online e funzionanti il prima possibile.

I piani di continuità aziendale di emergenza per un evento informatico devono essere ben documentati e regolarmente testati e aggiornati. La mancata risposta rapida a un evento informatico può essere un disastro sia dal punto di vista finanziario che della reputazione per un'azienda. Una polizza di assicurazione informatica svolge un ruolo importante in questo senso, non solo per il trasferimento del rischio, ma anche per l'accesso a competenze e servizi che aiutano le aziende a prepararsi ai rischi informatici, sia prima che dopo un evento.

Il tasso di sottoscrizione di assicurazioni informatiche da parte delle PMI (piccole e medie imprese) italiane è ancora relativamente basso: l'83% delle PMI italiane si ritiene immune da attacchi informatici e il 72% non ha mai seguito corsi di formazione informatica.

È importante che il mercato assicurativo dimostri alle PMI acquirenti il reale valore di una polizza informatica e che collabori con loro per innalzare gli standard di sicurezza informatica nelle loro aziende e nei vari settori industriali. Ciò comporterà non solo una cooperazione intersettoriale e un dialogo con i broker e gli altri esperti del settore assicurativo, ma anche una collaborazione con il governo e le agenzie di sicurezza.

Si tratta di una minaccia in continua evoluzione. È fondamentale che tutti noi facciamo il possibile per avere dei piani per valutare, mitigare e gestire il rischio, per trasferirlo dove possibile e per avere delle strategie per riprendersi dopo un evento.

di Luca Ricca