RISCHIO CYBER, BISOGNA GIOCARE D'ANTICIPO

TRA NUOVE TIPOLOGIE DI INSIDIE E POSSIBILI FRONTI DI FRAGILITÀ, L'ULTIMO CYBER CLAIMS REPORT DI COALITION LANCIA UN MESSAGGIO CHIAVE: LA PRINCIPALE FORMA DI DIFESA È QUELLA DI GESTIRE PROATTIVAMENTE OGNI POSSIBILE MINACCIA. LO STUDIO EVIDENZIA LE PRINCIPALI FONTI DI ATTACCHI INFORMATICI RILEVATI NEL 2024, PRIMO TRA TUTTI IL RANSOMWARE

di Beniamino Musto

Coalition è un insurance provider noto per il suo modello di "assicurazione attiva ideato per prevenire le minacce digitali prima che causino danni", come si legge sul sito della società. Ogni anno pubblica il proprio *Cyber Claims Report* con una mappa dettagliata sui trend degli attacchi cyber basati sui dati dei titolari di polizze sottoscritte negli Stati Uniti, in Canada, nel Regno Unito e in Australia.

L'edizione 2025 del rapporto evidenzia come le richieste di riscatto da attacchi ransomware nel 2024 siano diminuite del 22% su base annua, e l'importo medio è calato a 1,1 milioni di dollari, scendendo nel secondo semestre dell'anno scorso sotto la soglia psicologica del milione di dollari per la prima volta in due anni.

Ad ogni modo, il ransomware rimane la tipologia di attacco informatico più costosa e destabilizzante. La maggior parte dei risarcimenti per i sinistri aperti nel 2024 (il 60%) è dovuta a incidenti di compromissione delle email aziendali e frodi sul trasferimento di fondi, laddove il 29% degli eventi di compromissione della posta elettronica si è concluso con una transazione fraudolenta.

Inoltre, quasi il 29% degli incidenti riguardanti la compromissione di email aziendali ha portato a una perdita finanziaria attraverso trasferimenti fraudolenti, rendendo la compromissione della posta elettronica uno strategico punto di accesso per il furto di denaro. Il ransomware più frequente tra i clienti di Coalition nel 2024 è stato *Akira*, responsabile del 13% di tutte le denunce relative a questa tipologia di attacco, mentre *Black Basta*, coinvolto solo nel 3% dei claim, ha tuttavia pre-

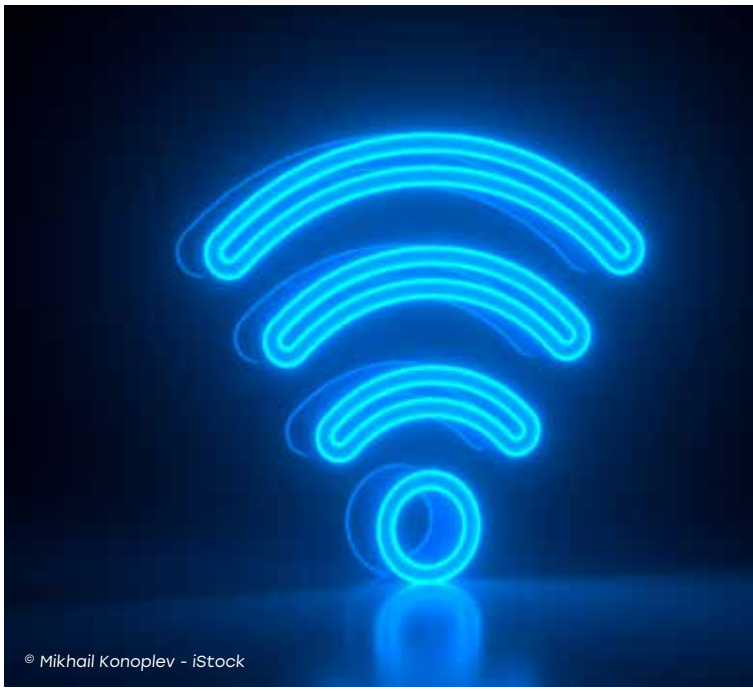
sentato le richieste di riscatto più elevate, con una media di 4 milioni di dollari.

NUOVE TIPOLOGIE DI EVENTI

Il Cyber Claims Report 2025 presenta due nuove tipologie di eventi: "perdite varie di prima parte" (miscellaneous first-party loss) e le "accuse di terze parti" (and third-party allegations). Ciascuna di queste categorie comprende una varietà di tipologie di eventi: le *perdite varie di prima parte* includono guasti di sistema, falle di sicurezza, violazioni di terze parti e altro; le *accuse di terze parti* includono violazione del copyright, impersonificazione di dominio, violazioni dei diritti alla privacy e altro.
Le accuse di terze parti si riferiscono a reclami presentati contro un'azienda da soggetti esterni a causa di un evento informatico, di una violazione della privacy, o di un errore che ha causato danni o responsabilità legali. Queste accuse sono spesso presentate da clienti, fornitori o enti regolatori e possono comportare cause legali, multe, controversie contrattuali e danni reputazionali. A differenza delle perdite di prima parte, le accuse di terze parti sorgono quando falle nella sicurezza, violazioni della privacy o controversie sulla proprietà intellettuale causano danni per altri: la terza parte subisce una perdita e cerca di ritenere un assicurato responsabile per i danni che ne derivano. Ciò può derivare da violazioni dei dati, divulgazione non autorizzata di dati personali, violazione o problemi di copyright relativi a contenuti digitali. La gravità delle denunce da parte di terzi nel 2024 è diminuita dell'86% su base annua, raggiungendo una perdita media di 23mila dollari.

UN IMPATTO DIVERSO A SECONDA DELLA DIMENSIONE

Quanto ai settori più colpiti, i più presi di mira sono i settori che gestiscono dati finanziari sensibili, informazioni sanitarie personali o proprietà intellettuale, a causa dell'elevato valore dei loro dati. Coalition riflette sul fatto che il rischio cyber ha un impatto diverso sulle aziende in base alle loro dimensioni, complessità e risorse a disposizione, fattori che influenzano direttamente l'esposizione complessiva delle aziende, i tipi di minacce che devono affrontare e la loro capacità di ripristino dopo un incidente. "Le Pmi – si legge nel report – spesso subiscono conseguenze finanziarie devastanti dagli attacchi informatici a causa delle risorse limitate e delle limitate competenze interne in materia di sicurezza. Le organizzazioni più


© Mikhail Konoplev - iStock

grandi, d'altra parte, possono disporre di programmi di sicurezza più sofisticati, ma subiscono attacchi altamente mirati a causa della loro vasta impronta digitale e del volume di dati sensibili in loro possesso".
Le richieste di risarcimento per ransomware hanno registrato un calo del 3% in frequenza e una riduzione del 7% in gravità, mentre i claim riguardanti i trasferimenti fraudolenti di denaro sono diminuitI del 2% in frequenza e del 46% in gravità, segnando un miglioramento significativo rispetto alle perdite record registrate nel 2023. A fronte di ciò, tuttavia, la gravità dei claim riguardanti la compromissione delle email aziendali è aumentata del 23%, evidenziando il crescente danno finanziario causato dalle comunicazioni aziendali compromesse.

STRATEGIE PER PREVENIRE IL DANNO

Quando si sono verificati attacchi ransomware, il 44% degli assicurati Coalition interessati ha scelto di pagare il riscatto quando ritenuto necessario. Secondo il rapporto, il team di *incident response* di Coalition ha negoziato riduzioni medie del 60% rispetto alle richieste di riscatto iniziali.
Uno degli aspetti più significativi del *Cyber Claims Report 2025* è quello che evidenzia come gli assicurati Coalition abbiano dovuto affrontare il 73% in meno di richieste di risarcimento per cybercrimine rispetto alla media del settore, un dato che l'azienda attribuisce al suo approccio proattivo alla gestione del rischio digitale.