

Gli attacchi sono sempre più costosi per le imprese di medie dimensioni in Europa, nonostante il calo dei volumi dei sinistri.

Milano, 23 settembre 2026 – La più recente analisi dei sinistri Cyber di Chubb rileva che mentre la frequenza degli incidenti informatici si è stabilizzata, l'impatto finanziario degli attacchi contro le imprese di medie dimensioni continua ad aumentare in modo significativo.

Le evidenze contenute nel [Chubb Cyber Claims Report 2026](#) mostrano che nel 2025, in Europa, la frequenza dei sinistri cyber delle imprese di medie dimensioni è scesa al livello più basso degli ultimi cinque anni, mentre il valore medio dei sinistri è triplicato tra il 2020 e il 2025.

Sebbene l'intelligenza artificiale aiuti le aziende a identificare e rilevare meglio le vulnerabilità informatiche, essa sta anche favorendo un uso malevolo della tecnologia sempre più sofisticato, con effetti che possono amplificare la velocità e l'ampiezza dell'esposizione al rischio.

Jimaan Sané, Head of Growth, Global Cyber di Chubb, ha affermato che per le piccole e medie imprese, una delle aree principali di esposizione è la supply chain aziendale, data la loro maggiore dipendenza da fornitori terzi.

“Le imprese di medie dimensioni si trovano sempre di più ad affrontare lo stesso livello di cyber disruption delle grandi aziende, ma spesso senza la stessa resilienza operativa”, ha dichiarato Sané. “Oltre a dover identificare e prevenire i propri guasti informatici quando sistemi, fornitori e partner interconnessi sono compromessi, le aziende devono affrontare anche le conseguenze finanziarie e operative.”

“Quando un fornitore tecnologico è colpito da un ransomware, le conseguenze raramente restano circoscritte. Per i retailer, i produttori e le aziende di servizi che dipendono dai sistemi di quel fornitore, l'impatto può essere immediato e grave: transazioni di vendita bloccate, visibilità dell'inventario persa e operazioni sospese. Anche se l'attacco ha origine all'esterno della loro organizzazione, la perdita da interruzione dell'attività ricade direttamente sul loro bilancio. Questa esposizione crescente evidenzia l'importanza cruciale di avere una copertura per l'interruzione dell'attività dipendente da terzi, all'interno di qualsiasi strategia completa di cyber risk”, ha aggiunto Sané.

Oltre alle minacce sempre più sofisticate guidate dall'AI e alla crescente dipendenza dalle supply chain, anche le frodi di social engineering, gli incidenti relativi alla privacy e gli attacchi ransomware continuano a rappresentare un rischio, secondo Chris Collier, Vice President Claims di Chubb.

“Questi tipi di incidenti possono essere devastanti, soprattutto per le piccole e medie imprese che non dispongono di un'adeguata copertura cyber e non hanno modo di recuperare o sostenere i costi delle perdite non recuperabili”, ha dichiarato Collier.

Gli attacchi ransomware, in particolare, continuano a rappresentare rischi significativi per le piccole e medie imprese, spesso con conseguenti data breach complessi e costosi. Anche quando i tentativi iniziali di cifratura sono sventati, l'esfiltrazione di informazioni sensibili può attivare ampi obblighi di notifica e interventi di ripristino.

“Chubb ha una notevole esperienza nella gestione dei sinistri ransomware e offre servizi altamente qualificati di supporto legale, informatica forense, pubbliche relazioni e altri servizi specialistici, per aiutare i clienti a rispondere agli incidenti e a gestirli senza intoppi, riducendo al minimo i tempi di inattività e favorendo il ritorno all'operatività”, ha aggiunto Collier.

Sul fronte difensivo, per rispondere a tali minacce e ridurre il rischio, le aziende e le organizzazioni possono implementare strumenti di mitigazione del rischio basati sull'AI, oltre a rafforzare la propria consapevolezza, considerando il cyber come una priorità del board e non solo come un progetto informatico.

Strumenti online come il [Chubb Cyber Index](#) offrono accesso in tempo reale a informazioni e risorse utili per aiutare le aziende a valutare e affrontare i rischi cyber. Chubb offre inoltre ai propri assicurati l'accesso a un'ampia gamma di strumenti e soluzioni, tra cui il supporto in ambiti quali la protezione cyber delle piccole imprese, la gestione degli incidenti e delle vulnerabilità, la sicurezza, strumenti di endpoint detection e response, la gestione del rischio privacy, la sicurezza e la consapevolezza degli utenti. Maggiori informazioni sono disponibili [qui](#).

Il **Chubb Cyber Claims Report 2026** è disponibile [qui](#).

Informazioni sulla Cyber Practice di Chubb

Chubb è leader nell'assicurazione del rischio cyber. Unendo una sottoscrizione di primo livello con servizi esperti di loss mitigation e di incident response di terze parti, offriamo polizze calibrate sulle esigenze e sui rischi specifici dei nostri clienti, per garantire che dispongano degli strumenti e delle competenze necessarie nel caso si verifichi un incidente cyber.

A proposito di Chubb

Chubb è un leader mondiale nel settore assicurativo. Presente in 54 paesi, Chubb offre soluzioni assicurative a imprese e individui in ambito Property & Casualty e Accident & Health a diverse tipologie di clienti. La compagnia si caratterizza per una vasta offerta di prodotti e servizi; una rete di distribuzione molto ampia; un'eccezionale solidità finanziaria; l'operatività a livello globale. Chubb Limited, la società capogruppo di Chubb, è quotata alla Borsa Valori di New York (NYSE: CB) e fa parte dell'indice S&P 500. Chubb impiega circa 45.000 persone nel mondo.

Media contact

Kathryn Coventry, Head of Communications EMEA, Chubb
kathryn.coventry@chubb.com