# PMI, LA MINACCIA DEL RANSOMWARE

di GIACOMO CORVI

SEMPRE PIÙ AZIENDE VENGONO COLPITE DA QUESTO GENERE DI ATTACCHI INFORMATICI. I COSTI DI GESTIONE E RIPRISTINO STANNO AUMENTANDO IN MANIERA VERTIGINOSA. SECONDO ALCUNI STUDI PUBBLICATI RECENTEMENTE, IL RISCHIO È ORMAI REALE E CRESCERÀ ANCHE NEL PROSSIMO FUTURO

© TomasSereda - iStock

Una donna ha fatto causa allo *Springhill Medical Center*, una struttura ospedaliera in Alabama, per la morte di sua figlia. La donna, come ha ricostruito il *Wall Street Journal*, si era recata in ospedale nel luglio del 2019 per dare alla luce una bambina. Durante il parto si erano tuttavia avute alcune complicazioni e la bambina, nata con un grave danno cerebrale, è deceduta dopo pochi mesi. Non si è trattato però di un semplice caso di responsabilità sanitaria: l'ospedale era stato colpito proprio in quei giorni da un attacco ransomware che aveva messo fuori uso la strumentazione tecnologica della struttura e reso inutilizzabili i macchinari per il monitoraggio del battito fetale, fondamentale per individuare tempestivamente qualsiasi complicazione durante il parto. La donna ha deciso di portare in tribunale l'ospedale perché, secondo la sua ricostruzione, non sarebbe stata informata adeguatamente sulle possibili conseguenze dell'attacco: in caso di condanna, ci troveremmo di fronte al primo caso accertato di morte da ransomware.

L'episodio, nella sua drammaticità, mostra la portata della minaccia ransomware in tutto il mondo. E costituisce l'ennesima prova (se mai ce ne fosse stato bisogno) che si tratta di un rischio reale. L'ultima conferma è arrivata di recente, con il *Cyber Claims Study* di **NetDiligence**: secondo il rapporto, gli attacchi ransomware sono i sinistri informatici che hanno provocato le perdite maggiori per le piccole e medie imprese.

## IL COSTO DI UN RANSOMWARE

Il rapporto, realizzato su un campione di circa 6mila sinistri informatici avvenuti fra 2016 e 2020, ha evidenziato che i ransomware hanno avuto un costo complessivo di 264 milioni di dollari per le piccole e medie imprese, pari al 40% delle perdite dovute ad attacchi informatici. Numeri che fanno del ransomware, come detto, la principale causa di esborsi per le Pmi, davanti ad hacker (29%), compromissione di mail aziendali (7%), phising (3%) ed errori commessi dal personale (0,5%). Gli attacchi ransomware si rivelano anche la ragione più frequente dei sinistri informatici: nei cinque anni presi in considerazione se ne sono contati quasi 1.500, ben al di sopra dei 441 episodi di attacchi hacker.

La richiesta media di riscatto è ammontata mediamente a 146mila dollari, mentre il costo complessivo del sinistro si è attestato a 179mila dollari. In entrambi i casi, i numeri hanno registrato una forte crescita negli ultimi due anni.

## I DANNI INDIRETTI DI UN ATTACCO

Gli effetti di un ransomware non si fermano tuttavia ai soli costi di gestione e ripristino. Il rapporto, per esempio, ha rilevato che il 79% dei sinistri di business interruption sono stati dovuti a un attacco ransomware. Fra il 2016 e il 2020 gli effetti di un blocco delle attività hanno avuto un costo medio di 975mila euro. Anche in questo caso si tratta di cifre in crescita negli ultimi anni: nel 2020 la perdita media per business interruption è arrivata a toccare quota 489mila dollari. Ingenti anche i costi per il ripristino delle infrastrutture tecnologiche a seguito dell'attacco. Il rapporto, a tal proposito, ha evidenziato che l'81% dei sinistri informatici che hanno richiesto spese di ripristino è stato dovuto a un ransomware. E che la perdita media nel quinquennio è arrivata a 49mila dollari. Inutile dire che, come rilevato in precedenza, si tratta di un trend in forte rialzo: nell'ultimo anno il costo medio per il ripristino delle infrastrutture informatiche è schizzato a 107mila dollari.

### LA SPINTA DEL CORONAVIRUS

Il coronavirus ha dato una forte spinta al fenomeno del cyber risk e, più nel dettaglio, del ransomware. Un recente studio di **Marsh**, intitolato *The changing face of cyber claims 2021*, ha evidenziato che i criminali informatici hanno saputo approfittare del "panico generato dalla pandemia di Covid-19": in alcuni casi, per esempio, gli hacker avrebbero persino imitato l'**Organizzazione Mondiale della Sanità** per avere accesso ai computer delle vittime. "Sono riusciti a sfruttare con grande successo la paura e l'incertezza associate al Covid-19", si legge nel rapporto. Seppur ancora minoritari rispetto al fenomeno complessivo del rischio informatico, questi episodi sono indicativi della capacità dei criminali del web di adattarsi e trarre vantaggio dalla situazione del momento.

## UN RISCHIO ANCHE IN FUTURO

Il rischio è dunque reale. Gli operatori del settore hanno iniziato a comprendere la portata della minaccia. E qualche segnale incoraggiante si comincia a vedere all'orizzonte. L'ultima edizione de *The State of Ransomware*, rapporto annuale curato da **Sophos**, ha per esempio evidenziato che soltanto il 37% delle imprese intervistate ha subito un attacco ransomware nell'ultimo anno: nell'edizione del 2020, giusto per avere un'idea, erano il 51% e il 54% in quella del 2007. Anche le difese delle aziende sembrano migliorate, con la quota di criptaggio dei dati che è passata dal 73% all'attuale 54%. Eppure, non si può ancora abbassare la guardia. Anche perché, accanto a dati incoraggianti, ci sono evidenze più sconfortanti. Nell'ultimo anno, tanto per citare un caso, è cresciuta la quota di chi ha deciso di pagare il riscatto richiesto per avere indietro i propri dati: erano il 26% nel 2020, adesso sono il 32%. Può sembrare una mossa sensata, visti anche i costi connessi al blocco delle attività e al ripristino del sistema, ma la scelta porta con sé anche qualche rischio. Innanzitutto perché pagare il riscatto in alcune giurisdizioni può costituire una fattispecie di reato. E poi perché non si potrà mai avere la certezza di avere i propri dati indietro: il rapporto di Sophos ha evidenziato che, in caso di pagamento, viene restituito soltanto il 65% dei dati che erano stati sottratti.

Le prospettive per il futuro non fanno dunque ben sperare. Per il 47% degli intervistati gli attacchi ransomware si stanno facendo più difficili da fermare. Il 40% giudica la minaccia persino inevitabile. E il 37% è convinto che altri settori industriali, magari trascurati in passato, diventeranno presto bersaglio dei criminali informatici.