LA POLIZZA CYBER TRA RANSOMWARE E CLAIMS MANAGEMENT

L'INCREMENTO ESPONENZIALE DELLA FREQUENZA E DELLA COMPLESSITÀ DEGLI EVENTI INFORMATICI AVVERSI HA CONDOTTO ALLA CRESCITA DELL'ENTITÀ DEI RISCATTI. PER QUESTO LA COPERTURA CYBER NON PUÒ PIÙ PRESCINDERE DA UNA CORRETTA MITIGAZIONE DEL RISCHIO. ECCO COME, SECONDO SHAM – GRUPPO RELYENS, GLI ASSICURATORI POSSONO ESSERE DETERMINANTI NELLA GESTIONE IN TEMPO REALE DELL'ATTACCO

Il *ransomware* è una particolare tipologia di *malware* (*malicious software*) che cripta dati e sistemi delle aziende, rendendoli di fatto inaccessibili, e che richiede il pagamento di un riscatto (ransom in inglese) per il rilascio della chiave di decifratura. I ransomware di ultima generazione, inoltre, prevedono un riscatto iniziale con possibilità di pagamento entro una breve finestra temporale (ad esempio una settimana), con minaccia, in caso di mancato pagamento entro quel termine, di un aumento esponenziale della richiesta di riscatto e di una pubblicazione nel web, nel *deep web* o nel *dark web* di dati personali, societari e segreti industriali la cui confidenzialità è stata violata dall'attacco stesso.

Luca Achilli, direttore sviluppo healthcare di **Sham** – gruppo **Reylens** e **Ruggero Di Mauro**, key account manager di Sham – gruppo Relyens, rispondono alle principali domande che riguardano l'efficacia delle coperture cyber per il settore sanitario.

Quanto è importante considerare il rischio cyber?

Luca Achilli: Gli attacchi ransom sono cresciuti in tutta l'Europa continentale, passando dal 14 al 32% di tutti gli eventi avversi cyber, e più che raddoppiando nel corso del solo 2020. Negli ultimi anni, si è registrato anche un netto incremento nell'impatto causato dagli attacchi hacker, come dimostra la violazione al Centro elaborazione dati e ai sistemi informatici della Regione Lazio. Il settore sanitario in Italia è vulnerabile. Secondo uno studio da poco pubblicato, su 20 strutture sanitarie pubbliche e private tra le 100 più grandi per fatturato o dimensioni, il numero di indirizzi mail compromessi dai quali può pervenire un attacco è, in media, di 353. Per compromesse si intendono le mail con password disponibili pubblicamente, utilizzate in passato per registrarsi su siti che abbiano subito un *databreach*.

Ci sono poi altri punti deboli. L'aumento dei ransomware è alimentato dalla pandemia e dai nuovi schemi ibridi *home/office working*. Eventi cyber avversi sono destinati ad aumentare sia in funzione della crescente digitalizzazione della sanità, sia della sofisticazione dei gruppi criminali. È essenziale che le organizzazioni investano in sicurezza cyber. La stessa tutela assicurativa offerta da una polizza cyber atta al trasferimento del rischio residuale, che è parte integrante di questo processo di *cyber resilience*, non può più prescindere da una corretta azione di mitigazione del rischio. Ciò significa che le compagnie assicurative hanno interesse a diventare partner di primo piano nella tutela cyber a 360°, offrendo con il prodotto assicurativo innovativi sistemi di prevenzione del rischio.

Come sta reagendo il mercato assicurativo?

L.A.: Si sta attraversando una fase di *hard market*: assistiamo, infatti, da una parte a un aumento dei premi

e delle franchigie minime giudicate sostenibili dagli assicuratori (e dai riassicuratori); dall'altro a una forte diminuzione della capacità assicurativa (massimale dispiegato dal singolo assicuratore per il cliente). Negli ultimi anni, infatti, malgrado la raccolta premi sia notevolmente aumentata, l'incremento degli eventi cyber avversi si è rivelato molto più che proporzionale. Ciò ha reso il mercato poco sostenibile nel lungo periodo con i tassi assicurativi, i massimali e le franchigie caratterizzanti la fase iniziale di diffusione del prodotto. Il mercato assicurativo, sempre più cauto nell'assunzione di *new business*, appare fortemente orientato nel garantire un rinnovo sostenibile del portafoglio esistente che porta a un repentino adeguamento delle condizioni di polizza. La direzione è quella di premi (tassi) sensibilmente più alti, franchigie più alte, massima esposizione della compagnia in termini di massimale centesimata e condizioni stringenti di rinnovo / assunzione, nonché sottolimiti, scoperti e coassicurazione del cliente richiesta per le garanzie più impattate da sinistri, ransomware *in primis*.

In che modo un assicuratore effettua la valutazione del rischio cyber?
Ruggero Di Mauro: Fino a qualche anno fa, per acquistare una polizza assicurativa cyber era sufficiente la compilazione di un semplice questionario assuntivo. Non erano previste *site visit* né approfondimenti tecnici particolari. Il processo assuntivo, oggi, è ben strutturato e prevede, generalmente, le seguenti fasi:

- compilazione di un questionario assuntivo generico, che analizzi le macrotematiche di organizzazione IT, sicurezza IT, rischio IT;
- compilazione di uno o più questionari specifici sulle aree esternalizzazione, Vpn, Mfa, formazione;
- *security call* e/o site visit e/o roadshow per l'analisi dettagliata e la consegna della *security roadmap* della proponente per i successivi 12/24/36 mesi;
- ricerca delle Cve (*common vulnerabilities exposures*) tramite piattaforme di big data in partnership con le compagnie assicurative e/o analisi non intrusiva degli indirizzi IP pubblici della proponente; dettaglio sul *remediation plan*;
- eventuali approfondimenti su eventi e sinistri precedenti all'assunzione o al rinnovo.

Quanto incidono la cultura e la consapevolezza di un'azienda nella stesura delle polizze?
R.D.M.: Le compagnie verificano una serie di variabili determinanti. Ad esempio, difficilmente rilasciano quotazioni a organizzazioni con sistemi informatici obsoleti e non aggiornati. Un altro livello di sicurezza

© solarseven – iStock

consiste nel sottoporre la struttura a un *rating* da parte di società esterne nell'ambito big data e *analytics*. È un'analisi molto approfondita per capire quali e quanti siano gli indirizzi informatici pubblici dell'azienda e se siano finiti nel mirino di attori terzi che operano nel dark web. All'azienda viene attribuito un punteggio per ciascuna categoria di rischio: nel caso in cui il punteggio risultasse negativo, si potrà stabilire di proseguire con approfondimenti *ad hoc* e richieste di azioni di miglioramento, oppure di non procedere alla quotazione e, di conseguenza, di non assicurarla.

Che ruolo ha l'assicuratore nella gestione di un attacco?
R.D.M.: Gli eventi cyber, per loro natura, presentano spesso una gestione complessa. Da un punto di vista assicurativo e di consulenza è determinante focalizzarsi sulla valorizzazione di un servizio di assistenza telefonica 24/7/365 che permette di avere un contatto immediato con esperti in ambito IT, legale e PR per avere una *second opinion* esterna. In questo senso, quindi, si concretizza una strategia *win-win* per la compagnia e per il cliente.

In conclusione, come una struttura sanitaria deve considerare la polizza cyber?
L.A.: Ci sono tre punti fondamentali da tenere a mente. Primo: la polizza cyber è il principale strumento di trasferimento del rischio cyber residuale, sempre sapendo che il rischio cyber non può essere portato a zero. Secondo: la polizza cyber non è un contratto da mettere nel cassetto. È uno strumento dinamico che fornisce supporto e assistenza tutti i giorni dell'anno. Per questo deve divenire parte integrante della governance sanitaria, integrandola ai piani di *disaster recovery, business continuity, incident management* e strutturando, insieme all'assicuratore, un efficace e tempestivo protocollo di gestione dei *claim*). Terzo: la polizza cyber è, per le analisi che precedono la sua stipulazione e per i meccanismi che genera la sua applicazione, uno strumento di mitigazione del rischio e di prevenzione.