UN GIOCO A GUARDIE E LADRI

di FABRIZIO AURILIA

È DIFFICILE PER IL MERCATO ASSICURATIVO ESSERE SEMPRE TECNICAMENTE AGGIORNATO SULL'EVOLUZIONE DEI SISTEMI DI ATTACCO INFORMATICO: ECCO IL PERCHÉ DELL'ATIPICITÀ DELLE POLIZZE CHE PROVANO A COPRIRE TALI RISCHI. NE ABBIAMO PARLATO CON GIANMARCO CAPANNINI, CYBER UNDERWRITER DI MUNICH RE

Il rischio cyber è percepito come una delle principali minacce emergenti ma lo si tende a considerare un mercato ancora di nicchia. Le polizze che coprono questo rischio saranno tuttavia tra le più diffuse negli anni che verranno. Ecco perché le compagnie si stanno attrezzando per rispondere a quello che sarà, potenzialmente, il futuro delle polizze danni. Ma la cosa non è semplice: asimmetria informativa, scarsa consapevolezza del pericolo e limiti di assicurabilità rendono la sottoscrizione di questo rischio una sfida aperta.

Gianmarco Capannini, cyber underwriter di **Munich Re**, società che si è mossa con anticipo su questo tema, anche grazie a una vasta esperienza internazionale, spiega a *Insurance Review* che le polizze cyber "sono prodotti assicurativi a copertura di danni immateriali derivanti da un attacco informatico. Questa tipologia di polizze forniscono solitamente copertura sia per i danni diretti all'assicurato sia per le richieste di risarcimento da parte di terzi".

TRA BUSINESS INTERRUPTION E DATA BREACH

Un attacco informatico può generare molteplici scenari che coinvolgono l'assicurato; per esempio, l'impossibilità dell'azienda di continuare a operare per un lasso di tempo. "In questo caso – dice Capannini – solitamente la compagnia fornisce il pronto intervento per il ripristino delle funzionalità del sistema informatico e delle banche dati, nonché il risarcimento dei danni indiretti derivanti dall'inoperatività dei sistemi. Particolari casistiche di attacco informatico, come l'estorsione (*vedi box a pag. 45*), prevedranno, inoltre, metodologie di ripristino specifiche".

Un altro scenario di particolare importanza è determinato dalla *copia* di dati personali sensibili; questa casistica è compresa nella polizza *Data breach* e può coinvolgere dati anagrafici, dati sanitari e dati afferenti a carte di credito. Le garanzie prestate sono di natura *liability* e tengono indenne l'assicurato da richieste di risarcimento e costi legali.

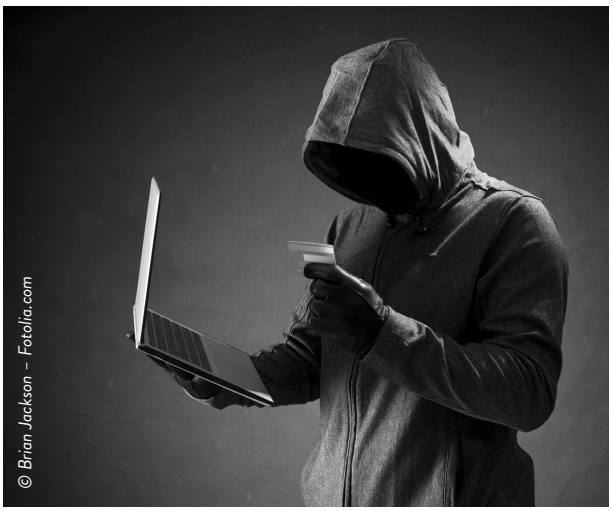
La maggior parte delle polizze include anche i costi di gestione dell'emergenza, danni reputazionali e costi di notifica, cioè quelli che l'assicurato deve sostenere per informare ogni soggetto di cui sono stati violati i dati personali. "I costi di notifica – sottolinea Capannini – possono essere rilevanti, in particolare per quei settori industriali che detengono un'ingente mole di dati sensibili. La nuova direttiva europea, che entrerà in vigore nel

2018 e che quasi tutti identificano come impulso principale del mercato, prevede oltretutto sanzioni rilevanti qualora chi subisca l'attacco non lo comunichi o non possa dimostrare di aver messo in atto tutte le misure tecniche per proteggersi".

CAPIRE L'ESPOSIZIONE PREVALENTE

Per gli assicuratori, nonostante vi siano segnali di sviluppo su tali prodotti, il mercato dei cyber risk resta un ramo molto complesso dove è difficile creare una strategia di ingresso e crescita. Secondo Capannini, è necessario capire per ogni settore industriale quale sia l'esposizione prevalente e valutarne il grado di rischio associato: "questa classificazione – sostiene – è assai complessa perché è necessario mappare l'insieme dei potenziali danni immateriali conseguenti all'attacco informatico. Ogni settore industriale è più o meno esposto sulle varie garanzie di polizza".

Pensando all'esempio della grande distribuzione, gli operatori di quel comparto sono più esposti di altri in termini di liability, costi di notifica e danni reputazionali; invece una società manifatturiera molto digitalizzata è più esposta a danni diretti propri, inclusa la mancata produzione. "Comprendere questo – commenta Capannini – è fondamentale per tarare massimali e franchigie coerentemente al bisogno dell'assicurato e alla corretta gestione delle esposizioni della compagnia".


© Brian Jackson – Fotolia.com

IL CRYPTOLOCKER NEMICO DELLE PMI

Il *cryptolocker* è la metodologia di attacco più frequente. È molto facile scaricare involontariamente un *malware* associato al cryptolocker che cripta i dati e sostanzialmente blocca la possibilità di operare, chiedendo un riscatto per la decriptazione. "La polizza assicurativa – spiega Gianmarco Capannini, cyber underwriter di Munich Re – gestisce la crisi e risolve il problema. In alcuni mercati, dove è consentito dalla legge, la compagnia paga il riscatto: in Italia questo, al momento, non è consentito".

Tale metodo estorsivo colpisce di frequente le Pmi. La funzione del cryptolocker è quella di guadagnare denaro tenendo in ostaggio il sistema operativo, ma nella stragrande maggioranza dei casi i dati vengono effettivamente decriptati al momento del pagamento del riscatto. "Uno dei problemi con questo tipo di malware – continua Capannini – consiste nel fatto che quando la vittima fa l'upload della password fornita dall'hacker per decriptare i dati, potrebbe scaricare anche un altro malware silente che permette di tenere aperta una porta d'accesso utilizzabile in futuro. La questione, sebbene su questa eventualità non ci siano certezze, pone però un problema di assicurabilità, perché – conclude – una Pmi su cinque è già stata colpita da cryptolocker e ha già pagato il riscatto".

LA SCELTA DEL PORTAFOGLIO

Altro tema da considerare è la dimensione delle aziende target. Per assicurare una grande impresa o una Pmi non occorrono polizze diverse, ma un prodotto modulare che è possibile adattare alle varie esigenze. Uno degli aspetti non ancora toccati, che cambia in base

alla dimensione dell'impresa, è la gestione del sinistro e i servizi da mettere a disposizione. "Le grandi aziende – spiega Capannini – hanno solitamente un *business continuity plan* e fornitori esterni già qualificati per la gestione dell'emergenza informatica: in questi casi l'assicuratore interviene attraverso periti specializzati che valutano i costi che l'azienda ha sostenuto. Le medie e piccole imprese in genere non sono altrettanto strutturate e si dovranno appoggiare ai servizi del service provider messo a disposizione con l'acquisto della polizza. L'assicuratore che vorrà concentrare il proprio interesse su questo segmento dovrà predisporre una serie di servizi di pronto intervento che includono la gestione dell'emergenza, gli aspetti legali e le *public relation*".
Portafogli che si basano prevalentemente su aziende corporate ci si aspetta siano esposti a sinistri rilevanti con tempi di ritorno relativamente lunghi; mentre se il portafoglio è composto essenzialmente da Pmi, è prevedibile che sia la frequenza il problema principale.

***Gianmarco Capannini**, cyber underwriter di Munich Re*


© wutzkoh – Fotolia.com

L'ASIMMETRIA INFORMATIVA

Ma l'impegno degli operatori potrebbe non bastare completamente. Capannini ritiene che uno dei problemi principali che deve affrontare l'assicuratore sia la profonda asimmetria informativa tra mercato assicurativo e conoscenza tecnologica. "È molto difficile per le compagnie – conclude – essere sempre tecnicamente aggiornate rispetto all'evoluzione dei sistemi e delle modalità di attacco informatico. Ecco perché questo prodotto è molto diverso dagli altri. La velocità di cambiamento della tecnologia informatica è molto più elevata rispetto all'evoluzione tecnologica negli altri ambiti industriali. Munich Re, in particolare, si è strutturata con tutte le risorse che possono fornire il valore aggiunto necessario per poter valutare gli aspetti di sicurezza informatica e di gestione del rischio con consapevolezza: tuttavia, tutti gli operatori devono essere consci del fatto che saremo sempre all'inseguimento delle evoluzioni tecnologiche".