# UN PRODOTTO CYBER NON BASTA

IN TERMINI DI SICUREZZA INFORMATICA, GRANDI AZIENDE, PMI E FAMIGLIE PRESENTANO ESIGENZE DIVERSE. SECONDO GIANMARCO CAPANNINI DI MUNICH RE, LE COMPAGNIE SONO CHIAMATE AD ANALIZZARE QUESTI BISOGNI PER COSTRUIRE UN'OFFERTA DIFFERENZIATA

Parlare semplicemente di *cyber risk* è forse obsoleto. Innanzitutto perché i *cyber attack* sono ormai soltanto una componente del più complesso rischio informatico, fatto di disattenzioni e semplici errori umani. E poi perché l'universo della protezione sembra diventato troppo ampio per poter essere ricondotto a una semplice etichetta: grandi aziende, Pmi e famiglie hanno bisogni diversi. Ecco perché non basta un semplice prodotto per costruire un'offerta.

"Il prodotto base è tendenzialmente sempre lo stesso: si tratta di una soluzione complessa, multi-line, capace di coprire eventi diversi che, al loro emergere, fanno scattare le garanzie", ha affermato **Gianmarco Capannini**, head of cyber & BB Bond di **Munich Re**. Pochi tratti in comune da cui deve partire la differenziazione dell'offerta.

## DALLE AZIENDE ALLE PMI

Già fra grandi aziende e Pmi c'è una certa differenza. "Nel mondo *corporate* – ha portato l'esempio Capannini – la fase di *pricing* deve essere supportata da software che consentano di integrare le informazioni raccolte con i classici questionari: solo così si può verificare, per esempio, se l'azienda ha già subito un *data breach*". Per le Pmi, viceversa, la più bassa capacità di spesa non consentirebbe di ripianare di costi d'acquisto di un simile software. In questo caso, secondo Capannini, la soluzione risiede in "questionari *tailor-made*, magari differenziati sulla base del tipo di azienda".

## SOLUZIONI PER LE FAMIGLIE

Se le soluzioni per le Pmi possono essere viste come versioni semplificate di quelle offerte alle grandi aziende, le famiglie sono proprio un mondo a parte: nessun rischio di *liability* o *business interruption*, ma bisogni più quotidiani come protezione contro le frodi informatiche e il *cyber-bullismo*. Anche la struttura cambia,


***Gianmarco Capannini**, head of cyber & BB Bond di Munich Re*

andando a configurare una soluzione quasi completa che possa accompagnare il cliente dal sinistro fino alla fase di ripristino. "È difficile pensare che una grande azienda, che magari ha già i suoi fornitori, consenta a un soggetto terzo di mettere mano ai suoi sistemi informatici quando avviene un sinistro", ha osservato Capannini. "Invece – ha aggiunto – per Pmi e famiglie la presenza di un *third service provider* può essere considerato un elemento a valore aggiunto".

## COME UN TERREMOTO

Qualche elemento in comune tuttavia c'è: l'esposizione a certi tipi di rischi. Già perché, com'è noto, gli attacchi informatici possono avere anche effetti pandemici, come avviene per i terremoti: *Petya* e *WannaCry*, in questo senso, hanno fatto scuola. "Il rischio di accumulo vale a prescindere dalle dimensioni", ha osservato Capannini. E per quanto manchino ancora modelli per tutti i tipi di rischio, le compagnie sono chiamate ad attrezzarsi per evitare l'emergere di un simile scenario. ***G.C.***