IL RISCHIO C'È, MA NON SI VEDE

L'OFFERTA NON MANCA, MA LE AZIENDE NON LA COMPRANO. L'AMBITO È VASTO, MA NESSUNO LO DELIMITA. QUESTO LO SCENARIO DEL CYBER RISK IN ITALIA, DOVE LE COMPAGNIE SI SCONTRANO CON UNA NORMATIVA POCO CHIARA, LA SCARSITÀ DI DATI SULL'ESPOSIZIONE DELLE IMPRESE E CLIENTI CHE NON PERCEPISCONO ANCORA LE REALI MINACCE

Il giro di affari prodotto dal *cyber risk* ha raddoppiato quello legato al traffico di droga. Eppure, nella quotidianità, si tende ad abbandonare le buone regole di *risk management*.

"Il mercato assicurativo – avverte **Cinzia Altomare**, branch manager **Gen Re** – potrebbe essere la prima vittima del cyber risk: con il progetto di dematerializzazione, l'**Ivass** ha imposto alle compagnie l'*home insurance*, riconoscendo a ogni assicurato il diritto di accedere ai propri dati via web. Gli assicuratori dunque, sanno bene l'importanza di tutelare i dati dei propri clienti".

Il cyber è una galassia che comprende una varietà di esposizioni e rischi *property*: dalla perdita degli elaboratori, al danno indiretto per il mancato funzionamento dei macchinari, fino alla responsabilità inerente il trattamento di dati (tutela del patrimonio aziendale e dei dati personali di terzi, danno reputazionale), a cui si applicano normative transfrontaliere che variano da Paese a Paese. "C'è una tale ampiezza di minacce ricondotti nel cyber risk – concorda **Umberto Rapetto**, cyber security advisor – che diventa difficile capire da dove cominciare. Siamo in presenza di una nebulosa che nessuno tenta di delimitare".

OFFERTA, A QUALE PREZZO?

A insistere su questo punto è anche la manager di Gen Re che sottolinea: "noi assicuratori siamo spesso accusati di non aver creato prodotti validi e specifici, ma il vero problema è che, se la normativa non è chiara e il perimetro non è ben definito, per le compagnie diventa

Cinzia Altomare,
branch manager Gen Re

Umberto Rapetto,
cyber security advisor

Luca Bolognini,
presidente Istituto Italiano Privacy

IL CASO BANCOPOSTA

Perdere i file sul disco senza aver fatto il *back up*, essere frodati al ristorante con la carta di credito, subire un furto di dati da un occasionale utilizzatore del nostro Pc. "In Italia – racconta Umberto Rapetto, cyber security advisor – questi episodi si raccontano poco per la paura di non trovare la stessa solidarietà che si riceverebbe nel caso del furto della propria auto. Un caso clamoroso, quello di **Bancoposta**, dove l'improvvisa scomparsa della virgola dalle operazioni di prelievo, ha depauperato il conto di chi, pur con 5.000 euro sul conto, si è visto negare prelievi di 200 euro.

difficile determinare il premio di una polizza". In Usa, il furto di dati produce, in media, 2,1 milioni di dollari con annesse spese legali di circa mezzo milione di dollari, ma in Italia, non vi sono dati certi. "Nel nostro Paese – conferma Altomare – soffriamo di una cronica ritrosìa, degli assicurati e delle compagnie, a parlare di numeri di danni subiti e, non avendo dati di mercato certi, diventa difficile costruire un'offerta. Innanzitutto, è necessario valutare il tipo di esposizione dell'azienda, ma, ad oggi, gli assicuratori non hanno dati sufficientemente attendibili per poter quantificare il costo della polizza e spingere l'offerta sul mercato."
A conferma di ciò, "alcune compagnie – sottolinea Rapetto – hanno lanciato prodotti senza conoscere la reale esposizione del soggetto ai rischi *corporate*. In questo senso, stiamo conducendo un esperimento di diagnostica, riferito a una qualunque organizzazione che dice di voler essere assicurata: in tre mesi, abbiamo individuato oltre 4.500 quesiti da fare alle imprese senza i quali non sarebbe possibile assicurarle".

INTRODUCIAMO L'RC OBBLIGATORIA

Tra gli ostacoli a un mercato che ancora non decolla, vi è, come si diceva, la normativa. "Io – suggerisce **Luca Bolognini**, presidente **Istituto Italiano Privacy**, e partner **Ict Legal consulting** – introdurrei l'obbligo di assicurazione anche nel *cyber crime*, proprio come nell'Rc auto: se le strade sono sempre più piene di automobili, allo stesso modo, le nostre vite sono sempre più fatte di dati. L'assicurazione obbligatoria, dunque, diventa un'ipotesi del futuro molto realistica". Ma con quali modalità? "Serve – spiega Bolognini – un approccio all'americana ovvero una settorializzazione, con direttive ad hoc per microcategoria (ad esempio la sanità elettronica). Se, invece, restiamo nell'ambito dell'assicurazione non obbligatoria, l'approccio può essere quello del macro perimetro, irrobustito da certificazioni che attestino la *compliance* a cui l'azienda si è attenuta".
Sul fronte dell'offerta, il passo da fare è una visione d'insieme. "Nel nostro mercato – conferma Bolognini – c'è la tendenza a vedere il cyber in modo scollegato da tutto il resto, offrendo prodotti *stand alone*. Se, invece, pensiamo che i dati non sono separati dal resto, ma incidono, sempre nel caso della Sanità, sulla presta-

zione sanitaria, diventa più facile spingere un'offerta che oggi fatica ancora a imporsi. Non ragioniamo sulla singola polizza, ma in una logica complessiva".
L'altro ostacolo allo sviluppo del mercato è la bassa percezione del rischio. "Le aziende – conferma Altomare di Gen Re – non percepiscono sufficientemente il rischio e il risultato è che le assicurazioni che propongono polizze per il cyber non hanno grandi risultati. La soluzione potrebbe essere partire da un ambito comune, uno zoccolo duro che valga per tutti, per poi specializzare l'offerta in base alle esigenze. Anche se, forse, siamo ancora troppo giovani per questo".

NON SOLO DIFESA, MA ATTACCO

La parola chiave, dunque, è sensibilizzare per elevare la percezione del pericolo. "È necessario – avverte **Marco Rossi**, head of sales & marketing di **Das Italia** – agire sulla prevenzione, promuovendo soluzioni di tutela legale, che, in caso di sottrazione e diffusione illecita di dati aziendali, intervengono, sul fronte civile e penale, aiutando l'impresa a recuperare credibilità". Le sanzioni interdittive possono essere rimosse con una buona polizza di difesa legale, che, a fronte di un costo contenuto (a partire da 170 euro), offre una copertura molto ampia sia per l'azienda sia per i suoi dipendenti. "Non basta difendersi – conferma Rossi – bisogna anche andare all'attacco: se un impiegato sottrae dati all'impresa, è importante promuovere una tutela legale nei suoi confronti, per evitare danni patrimoniali e reputazionali".
Recentemente Das ha introdotto *Difesa web*, una soluzione che aiuta a prevenire il furto di dati aziendali: imprese e singoli possono monitorare i propri dati, personali e finanziari, sul web per verificare un'eventuale sovraesposizione (se sono presenti su siti a rischio) o un rischio conclamato di furto di identità o frode creditizia. "Si tratta – spiega Rossi – di un servizio preventivo gratuito che Das offre per stimolare la domanda di un mercato di pura offerta come quello della tutela legale: il cliente ha l'immediata percezione del rischio e inizia ad adottare comportamenti virtuosi; questo si traduce in una riduzione dei sinistri (il 23% delle persone che abbiamo intervistato era già stato vittima di reato) e in premi meno cari".

Marco Rossi,
head of sales & marketing Das Italia

Sulla necessità di fare cultura, insiste anche Umberto Rapetto: "dobbiamo fare un po' di terrorismo, per evitare di arrivare all'11 settembre anche nel cyber: se assicuriamo l'auto, perchè non assicurare i dati che condizionano così tanto la nostra vita? Bisogna sensibilizzare i clienti e fare squadra per creare le condizioni di assicurabilità. Dobbiamo arrivare a dire: *ti assicuro se mi dai delle garanzie*; in questo modo l'assicurando si mette a posto e, alla fine del gioco, si alza il livello di attenzione. In questo, le compagnie dovranno assumere il ruolo di mentorship e tutorship in ottica di benessere globale". ***L.S.***