I BROKER E L'OPPORTUNITÀ DEL CYBER

di LAURA SERVIDIO

IN ITALIA, LA SENSIBILITÀ VERSO IL RISCHIO INFORMATICO CRESCE MA ANCORA POCO. SOLO IL 15% DELLE IMPRESE È COPERTO, NONOSTANTE OLTRE LA METÀ ABBIA SUBÌTO UN ATTACCO NEL 2017. UN FENOMENO IN AUMENTO, PENALIZZATO DA ALCUNE CRITICITÀ SUL FRONTE DELL'OFFERTA, A CUI IL GDPR CERCHERÀ DI RISPONDERE. QUESTI I TEMI DEL CONVEGNO NAZIONALE DI AIBA CHE SI È SVOLTO A ROMA

I danni complessivi provocati dal *cyber crime*, in Italia nel 2017, ammontano a circa 10 miliardi di euro. A essere sotto attacco sono soprattutto le grandi aziende e le organizzazioni governative, ma anche le piccole e medie imprese: oltre la metà di queste ha subito un attacco, lo scorso anno, per un costo medio unitario di circa 35 mila euro. Un fenomeno che preoccupa alla luce anche del fatto che un'azienda impiega mediamente 205 giorni per capire di essere sotto attacco.
Questo il *leit motiv* del convegno nazionale di **Aiba** dal titolo *Security code. I nuovi scenari per la gestione e il finanziamento del cyber risk nella industria 4.0, alla luce del Regolamento Gdpr,* dove, lo scorso mese gli attori del comparto hanno affrontato il tema da un punto di vista regolatorio, giuridico e di mercato.

Un momento del convegno

UN MERCATO EMBRIONALE

Il primo dato emerso è che la cultura di una gestione sistemica del cyber risk è in crescita nel nostro Paese, ma non abbastanza: una impresa e mezzo su 10 ha una copertura cyber (in Usa il rapporto è di uno a tre), per un valore di mercato di circa 30 milioni di euro. "Siamo ancora all'età della pietra", ammette **Maria Bianca Farina**, presidente di **Ania**, spiegando che l'attuale percezione del problema non è tale da far muovere l'offerta. Inoltre, le compagnie faticano a individuare standard di riferimento per un rischio in costante evoluzione, i cui costi totali sono difficili da stimare anche per la mancanza di dati storici.

LE CIFRE DEL FENOMENO

- I danni complessivi provocati dal cyber crime in Italia nel 2017 ammontano a circa i 10 miliardi di euro.
- Oltre il 50% delle Pmi ha subito un attacco (nel 2017), per un costo medio unitario di circa 35 mila euro.
- Il mercato assicurativo italiano cyber è ancora in fase embrionale: circa 30 milioni di euro in coperture.
- Circa quattro miliardi i record compromessi e le informazioni rubate.
- Otto miliardi gli oggetti connessi alla rete che, entro il 2020, si stima diventeranno 20 miliardi.

LAVORARE INSIEME

A dare una speranza è il *Regolamento generale sulla protezione dei dati (Gdpr)*, in vigore negli Stati Ue dal prossimo 25 maggio, che aiuterà ad aumentare la sensibilità di cittadini e imprese verso questo tema, obbligando tra l'altro gli imprenditori a denunciare gli attacchi subiti. In questo, i broker giocheranno un ruolo fondamentale sia nella diffusione della cultura del rischio sia nell'individuazione delle strategie di mitigazione: l'unica strada per la messa in sicurezza del patrimonio aziendale.
Per gli intermediari, quindi, si apre una grande opportunità, come evidenzia anche la rappresentante delle imprese assicurative. Il cyber richiede un'alta capacità consulenziale che da sempre caratterizza i broker e qui l'invito delle compagnie è a lavorare insieme visto che assicuratori e intermediari sono gli unici ad avere le competenze, gli strumenti e la cultura per valutare il rischio cyber.

UNA VORAGINE NELLA PROTEZIONE

Il problema, però, si sposta nuovamente sul fronte dell'offerta. In generale, la polizza cyber può coprire sia i danni dell'impresa, sia i danni a terzi, sia i costi per la difesa legale, ripristino, reputazione e altro. Attualmente però, osserva il presidente di Aiba, **Luca Franzi De Luca**, si sta affermando la tendenza a escludere, da un lato, il cyber risk dalle coperture tradizionali (property & casualty) e, dall'altro, le lesioni e i danni materiali dalle polizze cyber: una carenza che rischia di creare "voragini nella protezione".

Su questo interviene anche il regolatore che evidenzia i principali requirement delle polizze cyber le quali, ammette **Pietro Franchini**, servizio studi e gestione dati **Ivass**, "non possono coprire tutto". Il problema è valutare il rischio residuo e fare un buon pricing. Ma soprattutto le polizze devono spiegare con chiarezza e trasparenza quali sono le garanzie incluse ed escluse e soprattutto devono essere corredate da servizi accessori di gestione del rischio e della crisi.

PERSONALIZZAZIONE E INTEGRAZIONE

Su un fatto tutti gli intervenuti concordano: la polizza non può essere la panacea di tutti i mali. Non esiste un'unica soluzione, ma "la soluzione per quel cliente", spiega Franzi De Luca, a cui si può giungere dopo un'attenta analisi delle potenziali minacce e la definizione del perimetro dei rischi da trasferire.

Approccio personalizzato, quindi, ma non solo. Secondo i partecipanti al dibattito è necessario andare verso una strategia integrata: l'unica pensabile, sostiene anche **Alessandro De Felice**, presidente di **Anra**, in cui soluzioni innovative possono arrivare anche dal mondo non assicurativo. L'opportunità da cogliere sta nella trasformazione della vendita in una consulenza di valore, in una logica di integrazione del servizio con la componente assicurativa. E in questo potrà venire in aiuto la normativa: la Gdpr rappresenta l'opportunità per entrare in un discorso cyber integrato che permei tutta l'attività, nella consapevolezza che la copertura non potrà mai coprire l'intero rischio.

CAMBIO DI PARADIGMA

Il nuovo regolamento inoltre, secondo **Stefano Mele**, avvocato presso **Carnelutti Studio Legale Associato**, sarà utile anche per capire in che modo gli altri rischi vengono presidiati, gestiti, mitigati e conosciuti. Ma sarà necessario un cambio di paradigma che sposti il focus dal concetto di privacy a quello di protezione dei dati personali: solo cambiando questo punto di vista potrà nascere l'esigenza di *compliance*, giustificando lo sforzo che le aziende devono compiere per adeguarsi. Tra l'altro, proprio l'essere compliance, aggiunge **Francesco Teodonno**, security unit leader di **Ibm Italia**, agevolerà quel salto culturale che vede nella risorsa umana il vero protagonista: non basta comprare software e tool, servono figure che li sappiano gestire e i dati dicono che sono necessari 20 milioni di risorse lavorative per affrontare il cyber a livello globale.

La prospettiva, dunque, è ampia, anche se resta il problema della domanda: "il cliente non è ancora pronto ad investire in polizze cyber", conclude il presidente di Aiba, e i broker sono impegnati in questo salto culturale sia come operatori qualificati del mercato che nei rapporti con il regolatore, "per far sì che questa opportunità non vada sprecata".