CYBER RISK, TRA LUCI E OMBRE

di LAURA SERVIDIO

CRESCE IL LIVELLO DI CONSAPEVOLEZZA DEL RISCHIO INFORMATICO E DELLA NECESSITÀ DI PROTEZIONE DEI DATI DELLA CLIENTELA. MA RESTANO IL PROBLEMA CULTURALE E I LIMITI SULLA FORMAZIONE. COME EMERGE DA UN'INDAGINE IVASS, PRESENTATA A ROMA NEL CORSO DELL'INIZIATIVA INSURTECH

Siamo nell'epoca del *consumer 4.0*: un soggetto nuovo che amplia i luoghi e le scelte di acquisto ponendo sfide e minacce emergenti. "È il segno di una nuova geografia del consumo, in cui mobilità e comunicazione soddisfano bisogni istantanei". A sottolinearlo è **Maria Luisa Cavina**, responsabile del servizio vigilanza intermediari assicurativi dell'**Ivass**, nel corso di *Insurtech*, un'iniziativa promossa dal Regolatore lo scorso dicembre per stimolare un confronto con imprese e intermediari in merito all'impatto che l'innovazione ha sul mercato assicurativo.

In particolare, le polizze di *digital micro insurance* e i prodotti *pay per use* pongono sfide per la vigilanza, tanto in termini di adeguatezza e trasparenza, quanto di esposizione al rischio informatico.
Su quest'ultimo fronte, lo scorso luglio l'Ivass ha realizzato un'indagine conoscitiva sui presidi degli intermediari tradizionali per la gestione delle informazioni e la prevenzione dei rischi informatici. Un questionario di 20 domande è stato sottoposto a 2900 intermediari (200 broker e 2700 agenti), tramite le associazioni di categoria: il quadro emerso rivela un discreto livello di consapevolezza sul cyber risk e sulla necessità di protezione dei dati della clientela.

TRA PLUS E MINUS

In particolare, oltre l'80% degli intermediari dice di adottare presidi di base per fronteggiare il rischio informatico, prevalentemente attraverso l'utilizzo di password alfanumeriche, sistemi e reti protetti da accessi non autorizzati, e periodici back up di dati.

Un'evidenza positiva che nasconde, però, anche ombre. Ad esempio, solo il 20% degli intermediari (e il 50% dei grandi broker) adotta policy aziendali in materia di cyber risk e test anti intrusione, il 40% degli agenti (il 50% dei broker e il 90% dei grandi broker) ricorre a sistemi e strumenti di analisi dei rischi, e solo il 22% fa rilevazione degli accessi non autorizzati.

***Maria Luisa Cavina**, responsabile del servizio vigilanza intermediari assicurativi dell'Ivass e **Salvatore Rossi**, presidente dell'Ivass*

Non solo. Si registra una carenza sul fronte culturale. In particolare, l'impatto del Regolamento Ue 2016/679 (data protection) è stato valutato da appena il 30% degli agenti (dal 50% dei broker e dal 70% dei grandi broker) e solo il 50% (e il 60% dei broker) ha fornito informazioni di base al personale; percentuale che scende al 23% per gli agenti (al 30% per i broker e l'80% per i grandi broker) nel caso della formazione specifica, evidenziando una scarsa valutazione del fattore umano nel contenimento del rischio informatico. Basso anche il ricorso allo strumento assicurativo per il rischio residuo, previsto dal 10% degli agenti, dal 12% dei broker e dal 40% dei grandi broker.

LINEE GUIDA PER IL CAMBIAMENTO

In sintesi, "vi sono ampi margini di miglioramento", ha osservato Cavina. Un processo che il regolatore vuole promuovere fornendo agli intermediari indicazioni sugli interventi e sulle iniziative di potenziamento dei propri presidi, favorendo un rapido ed efficace processo di autovalutazione e di autocorrezione. Seguendo due direttrici: la prevenzione e la protezione dei dati.

UN RISCHIO SOTTOVALUTATO

Il cyber è un'area su cui il sistema produttivo italiano investe ancora poco (4.500 euro, con punte di 19mila euro per il settore Ict), nonostante il 45% delle imprese manufatturiere e dei servizi finanziari abbia subito un attacco informatico.
Secondo un ricerca condotta da Banca d'Italia sul rischio informatico, nel periodo settembre 2015 - settembre 2016, solo il 13,5% delle imprese Ict e il 4,8% di quelle a bassa tecnologia hanno stipulato polizze stand alone, mentre ben il 59,3% delle prime e l'81,5% delle seconde non risulta assicurato. A non spendere nulla è il 20% delle imprese, ma il 12,9% dichiara di non aver trovato sul mercato una copertura adeguata.

***Maria Luisa Cavina**, responsabile del servizio vigilanza intermediari assicurativi dell'Ivass*

Sul primo fronte, l'Istituto raccomanda che gli intermediari adottino specifiche policy su cyber risk e data protection, definite con le rispettive associazioni di categoria, da condividere con i propri collaboratori e dipendenti; ma anche che accrescano le conoscenze informatiche, proprie, dei collaboratori e dei dipendenti, destinando a questo aspetto una percentuale del monte ore biennale di aggiornamento professionale.
Sul piano della protezione, la raccomandazione riguarda l'innalzamento della sicurezza dei sistemi, il potenziamento del monitoraggio contro accessi non autorizzati, l'aumento della frequenza dei test anti-intrusione e dei backup dei dati, e l'adozione di un piano di gestione di eventuali crisi.
Ultimo punto, ma non per importanza, l'ampliamento del ricorso allo strumento assicurativo per la copertura del rischio residuo. "Il mercato italiano – ha sottolineato Cavina – è ancora in una fase embrionale". Su questo fronte, l'Istituto auspica lo sviluppo dell'offerta di protezione.

PROSSIMI STEP

Infine, la lettera al mercato di prossima emanazione, in cui l'Istituto illustrerà i risultati dell'indagine sul cyber risk, dovrà fornire agli operatori le indicazioni ritenute fondamentali per una significativa mitigazione dei rischi. Entro il 2019 l'Ivass ripeterà l'indagine, per valutare il grado di adesione alle misure suggerite e misurare il livello di evoluzione del settore in materia di sicurezza informatica e di resilienza agli attacchi informatici.