Insurance Daily

MARTEDÌ 6 DICEMBRE 2016 N. 1039

PRIMO PIANO

Vita, un 2017 di volatilità

L'agenzia di rating Moody's ha abbassato a *negativo* (da *stabile*) l'outlook 2017 del settore assicurativo vita a livello globale. Il giudizio è stato determinato alla luce della persistenza dei bassi tassi di interesse e dell'aumento della volatilità dei mercati finanziari. Secondo Moody's, l'incertezza dei mercato "non solo aumenta la volatilità degli utili da commissioni delle compagnie, ma scoraggia anche quei detentori di polizze avversi al rischio ad acquistare prodotti senza garanzie". Ad appesantire lo scenario, osserva l'agenzia di rating, sono poi i cambiamenti normativi negli Usa e in Europa, che stanno fermando la vendita dei prodotti esistenti e controbilanciando i benefici derivanti dalla stabilizzazione della crescita economica e dal calo della disoccupazione. Moody's vede anche un possibile aumento di fusioni e acquisizioni nel settore vita, considerato che le compagnie stanno cercando di liberare capitale e ridurre i costi. Secondo Benjamin Serra, vice presidente e senior credit officer di Moody's, "nonostante i sobbalzi dopo l'elezione presidenziale Usa, i tassi d'interesse a livello storicamente basso resteranno il principale rischio per le compagnie vita globali nel 2017, continuando a deprimere i rendimenti degli investimenti e la redditività".

Beniamino Musto

RISK MANAGEMENT

Cosa cambia nel trattamento dei dati

Per far fronte agli attacchi Cyber e rispettare le disposizioni del nuovo regolamento europeo è opportuno fare ricorso a procedure di risk management e certificazioni di qualità. In questo contesto, PA e aziende private italiane risultano tra le più vulnerabili

(SECONDA PARTE)


© Andrey Popov - Fotolia.com

Come è stato anticipato nella prima parte di questo articolo, il *Titolare* deve effettuare una valutazione dell'impatto del rischio *privacy*, o ***Privacy Impact Assessment*** (PIA), fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, in tutti i casi in cui il trattamento presenti rischi specifici per i diritti e le libertà degli interessati.

Il PIA deve quindi prevedere:

1. l'analisi dei rischi;
2. l'identificazione delle eventuali problematiche per la loro corretta gestione;
3. l'*Action Plan* previsto per la risoluzione di tali problemi;
4. il controllo annuale degli interventi effettuati per ridurre i rischi.

In caso di violazione, il Titolare ha l'obbligo di darne nota al *Garante* entro 72 ore dal fatto e, qualora la violazione stessa possa comportare dei danni per i diretti interessati, di segnalarla anche a questi ultimi senza ritardo.

La questione non è di poco conto: secondo uno studio del **Ponemon Institute**, occorrono in media 205 giorni per identificare una falla nei sistemi di sicurezza e molti soggetti si rendono conto dell'avvenuta violazione solo dopo che gli autori della stessa si sono fatti avanti con eventuali tentativi di estorsione.

Nel luglio del 2014, ad esempio, un attacco di hacker alla **Bce** ha causato la sottrazione di migliaia di indirizzi e dati personali di cittadini europei: questo attacco, però, è stato scoperto solo quando gli autori hanno contattato la banca per chiedere un riscatto.

Inoltre si stima che ogni giorno vengano scoperti più di 300 mila varianti di *malwares*, ovvero di programmi creati con lo scopo di eseguire attacchi specifici per distruggere dati, rubare informazioni e perfino compromettere l'attività delle vittime.

(continua a pag. 2)

Insurance Daily

MARTEDÌ 6 DICEMBRE 2016 N. 1039

(continua da pag. 1)

SANZIONI PESANTI

Gli obiettivi degli attacchi, infatti, possono essere disparati, dalla semplice *diffusione* (accesso ai sistemi per propagazione massiva, come accade per lo *spam*), al *cybercrime* (furto di dati per trarne vantaggi politici, economici o finanziari), dall'*hactivism* (diffamazione di organizzazioni o divulgazione di dati riservati) al *furto di identità* (sottrazione di informazioni personali dei cittadini), fino al danneggiamento vero e proprio degli affari di una compagnia, in seguito a *distruzione o cancellazione* dei suoi dati.

Una tale varietà e complessità di intenti rende estremamente difficile l'individuazione tempestiva degli attacchi e costituisce ora un serio pericolo per il Titolare del trattamento, se non dovesse denunciarli nei tempi previsti.

Le sanzioni applicate dai Garanti in caso di perdita dei dati, infatti, diventano molto più significative:

- fino a 20 milioni di euro per i privati e per le imprese non facenti parte di gruppi;
- fino al 4% del fatturato consolidato complessivo per i gruppi societari.

Si tratta di importi molto cospicui, giacché queste ammende sono pensate per incidere sulla condotta dei grandi gruppi che trattano dati in diverse aree geografiche e spesso cercano di individuare veri e propri paradisi legali, per eludere le norme e i criteri definiti dalle nazioni più rigorose sul trattamento dei dati personali.

SERVONO MODELLI ORGANIZZATIVI EVOLUTI

Attraverso l'imposizione del *Privacy Impact Assessment* le Autorità di controllo incoraggiano l'istituzione di meccanismi di gestione del rischio e di certificazione delle procedure per la protezione dei dati, allo scopo di dimostrare la loro conformità al Regolamento.

L'adesione a un codice di condotta o a un meccanismo di certificazione approvato può dunque essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza. È sempre più evidente, infatti, come i dati personali costituiscano una nuova materia prima in grado di generare ingenti guadagni o perdite per le imprese, e che va dunque gestita con modelli organizzativi evoluti ed efficienti.

In particolare i Titolari possono iniziare il percorso preparatorio alla certificazione, sottoponendo le loro aziende a valutazioni dei processi sulla base di protocolli di certificazione già esistenti, come il protocollo *BSI:10012* per la gestione delle informazioni personali, che realizza processi per la corretta gestione della privacy, o il protocollo *EuroPriSe* (European Privacy Seal), basato sulla direttiva 95/46.

PIÙ SICURI SE C'È FORMAZIONE

Un'efficace strategia di protezione e mitigazione dei rischi inizia sempre dalla formazione.

Oggi più che mai, infatti, sono gli utenti a rappresentare l'anello debole della sicurezza, all'interno di un'organizzazione.

Secondo uno studio di **Microsoft**, il 23% dei messaggi elettronici contenenti tentativi di *phishing* (tipo di truffa, attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale) viene aperto. (continua a pag. 3)

Insurance Daily non uscirà dal 7 al 9 dicembre

A Milano domani si festeggia il Santo patrono, Sant'Ambrogio, ed è festa. E poi si fa il ponte

Insurance Daily non uscirà da domani, 7 dicembre, a venerdì 9. Quindi l'appuntamento con il quotidiano del settore assicurativo sarà per lunedì 12 dicembre.

Anche il sito *Insurancetrade.it* non sarà aggiornato in questi giorni, poiché la redazione di **Insurance Connect**, avendo la propria sede a Milano, resterà chiusa da domani, unendo alla festa di Sant'Ambrogio, patrono della città, quella dell'*Immacolata Concezione* e venerdì 9, concedendosi un piccolo *ponte*.

Tutte le attività ripartiranno lunedì 12 dicembre.

A tutti i lettori buon ponte (qualora lo facciate) e ai milanesi: buon Sant'Ambrogio.

(continua da pag. 2)

L'11% delle vittime apre quindi il *link* solitamente allegato in questi messaggi, concedendo di fatto pieno accesso agli hacker: nel 60% dei casi l'attacco ha successo in pochi minuti.

Sfortunatamente, infatti, la maggior parte delle aziende usano metodi antiquati per rilevare le *infezioni da malware*, in quanto la maggior parte dei sistemi sono configurati in modo da consentire l'esecuzione di un processo informatico prima ancora che il sistema di monitoraggio (basato sul riconoscimento della firma o *impronta* del malware) rilevi l'evento come un attacco.

In pratica, solo dopo l'entrata in funzione del malware, il sistema anti-malware interviene per ripulire il computer e assicurarsi che l'infezione non si ripeta. Questa è la ragione principale per cui, secondo **Symantec**, gli antivirus sarebbero oggi in grado di individuare non più del 45% degli attacchi provenienti da hacker.

C'è da notare, inoltre, che questi ultimi eseguono sempre più spesso attacchi di tipo avanzato, definiti *Advanced Persistent Threats* (APT o minacce persistenti avanzate), grazie ai quali, una volta entrati nella rete bersaglio, ne sfruttano gli strumenti di sistema e persistono al suo interno anche per anni, rendendo estremamente difficili e costosi i processi di *disinfezione*.

LO STATO DELL'ARTE IN ITALIA

La situazione nel nostro Paese risulta essere particolarmente grave.

Uno studio effettuato nel 2014 dal **Ponemon Institute** sulle violazioni dei dati in Italia, ha rivelato come il settore pubblico e quello delle aziende private di vendita al dettaglio siano quelli con la probabilità più alta di accadimento stimata. È possibile che una spiegazione di questo fenomeno risieda nella maggiore quantità di informazioni riservate e sensibili raccolte da questi settori, in combinazione con un livello generalmente inferiore di sicurezza. Per contro, i settori che trattano energia e trasporti sembrano beneficiare di una più bassa probabilità di accadimento.

Secondo il *Cyber Intelligence and Information Security Center* dell'**Università La Sapienza** di Roma, che ha condotto una ricerca a livello nazionale, tutte le organizzazioni finanziarie risulterebbero essere state attaccate, e le violazioni avrebbero avuto successo nel 17% dei casi, grazie all'elevato grado di sicurezza che caratterizza i sistemi di banche e istituti di credito in genere.

La Pubblica Amministrazione, invece, conterebbe il maggior numero di attacchi riusciti (62%), il che confermerebbe l'adozione di politiche di sicurezza insufficienti.

Il settore industriale resterebbe il meno aggredito, ma solo il 29% delle aziende sarebbe in grado di rilevare minacce persistenti avanzate (APT).

Quale futuro possiamo dunque immaginare per la sicurezza della privacy nel nostro Paese?

A prescindere dall'obsolescenza dei sistemi e delle politiche adottate, c'è da rilevare che, in generale, la superficie di attacco complessivamente esposta dalla nostra civiltà digitale sembra crescere assai più velocemente della nostra capacità di proteggerla e che i sistemi di difesa impiegati non riescono a essere abbastanza efficaci. Pure a fronte di crescenti investimenti nella sicurezza informatica, infatti, il numero degli attacchi continua ad aumentare.

In tale contesto, in cui peraltro si stima che gran parte degli incidenti non vengano nemmeno rilevati dalle vittime, si innesta il nuovo Regolamento europeo per la salvaguardia dei dati personali, una normativa articolata e complessa che impone alla quasi totalità dei soggetti giuridici che operano nella nostra società, siano essi privati, aziende o enti pubblici, di operare con un approccio completamente integrato per il trattamento dei dati personali, non più basato sul semplice concetto di *compliance* ma caratterizzato da un'attenta analisi e gestione dei rischi determinati dal nostro vivere quotidiano nella civiltà digitale.

Cinzia Altomare

(La prima parte dell'articolo è stata pubblicata su Insurance Daily di ieri, lunedi 5 dicembre)

Insurance Daily

MARTEDÌ 6 DICEMBRE 2016 N. 1039

INTERMEDIARI

Fpa, sedici risposte per trattenere gli iscritti

Il fondo pubblica un documento per rispondere alle domande più frequenti che giungono dagli intermediari dopo la ripresa delle attività ordinarie

Il **Fondo pensione agenti** ha pubblicato un documento, *Sedici domande al Fondo pensione agenti*, che ha l'obiettivo di rispondere ai quesiti più frequenti che arrivano agli amministratori dopo la ripresa delle attività ordinarie, in seguito al lungo commissariamento terminato a novembre scorso.

Attraverso alcune risposte a domande precise, in modalità *Faq*, gli amministratori di Fpa ribadiscono che il fondo resta, si legge in una nota, "il più conveniente e vantaggioso per gli iscritti, perché garantisce una pensione più elevata, a minor costo per chi aderisce, anche grazie al contributo delle compagnie che, invece, non sussiste negli altri fondi". I cambiamenti tecnici voluti dalla **Covip**, continua la nota che accompagna il documento, "hanno determinato una stabilità duratura nel tempo e il bilancio tecnico del 2015 registra un attivo di 42 milioni di euro".

Rispondendo alle domande più frequenti degli iscritti al fondo, o anche ai semplici agenti interessati, Fpa mira da un lato a trattenere gli iscritti, scongiurando un'eventuale trasferimento ai fondi aziendali, e dall'altro a favorire l'adesione di nuovi intermediari.

La prestazione definita, ricorda Fpa, permette di beneficiare di prestazioni accessorie (assegni di invalidità e reversibilità), che invece in uno strumento a contribuzione definita (come quelli privati gestiti dalle imprese) sarebbero "a pagamento". I fondi aziendali non sono certo immuni alle crisi finanziarie: risentono dell'andamento della gestione finanziaria della singola impresa, il che può influenzare le pensioni "che in caso di crisi potrebbero ridursi rispetto alle aspettative".

Le prime domande sono le meno interessanti, perché ripercorrono la storia del disavanzo prospettico che ha portato al commissariamento di Fpa: quando è emerso per la prima volta il disavanzo prospettico? Gli amministratori hanno preso provvedimenti? Perché Fpa si è trovato in squilibrio? Perché è stato commissariato?

Prevista l'uscita di 4000 iscritti

Poi il documento entra nel vivo degli aspetti che interessano maggiormente sia chi è iscritto al fondo ma magari ha interrotto i versamenti, sia chi è tentato dal trasportare il proprio tesoretto in un Pip di una compagnia, sia per l'agente che vorrebbe iscriversi ma non è sicuro che il fondo sia solido.

Gli amministratori, quindi, assicurano che le misure contenute nel piano approvato dalla Covip hanno riportato Fpa in equilibrio. "Dopo aver raggiunto l'equilibrio – si legge – sono state costituite attività supplementari pari al 4% delle riserve tecniche. La legge prevedeva che potessero essere impiegati 10 anni per costituire le attività supplementari ma la Covip ha stabilito che nel caso del fondo agenti il 4% di margine di garanzia dovesse essere disponibile da subito. Ulteriore elemento di garanzia è costituito dal fatto che, per tenere in considerazione la possibile uscita volontaria degli aderenti dopo l'applicazione dl piano, è stata introdotta una previsione estrema che possa consentire il mantenimento dell'equilibrio anche nell'ipotesi che il 30% degli aderenti abbandoni il fondo".

Ma qualora le richieste di trasferimenti e riscatti fossero superiori al 30%? Aumenterebbe chiaramente il fabbisogno: il 30% (pari a circa 29 milioni) corrisponde a un onere già conteggiato nel bilancio tecnico di riequilibrio. A oggi, gli agenti iscritti sono circa 13 mila; secondo Fpa è "poco realistica la possibilità che escano più di 4.000 iscritti" perché, sostengono, la permanenza in Fpa è ancora conveniente.

Gli amministratori rassicurano anche dal punto di vista del tasso di attualizzazione delle riserve tecniche del patrimonio ipotizzato nel piano di riequilibrio, che è fissato al 3,5% annuo. Ricordano che la media della serie storica dei rendimenti di Fpa è superiore al 3,5% (la media 2015 e 2016 si attesterà sopra il 7% annuo). "Inoltre – scrivono – poiché c'è un margine di circa 200 milioni di euro dato da plusvalenze non realizzate, nei prossimi anni il 3,5% di rendimento potrà essere raggiunto non solo con la redditività corrente ma con l'utilizzo di parte delle stesse plusvalenze".

Infine, l'ultima domanda è dedicata a chi ha sospeso l'iscrizione e vuole riprendere i versamenti: occorrerà inviare una richiesta agli uffici del fondo entro il 31 dicembre per poter ancora porre a carico dell'impresa la quota per l'anno in corso. Per le quote arretrate è prevista comunque una rateizzazione.

Fabrizio Aurilia

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 6 dicembre di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577