Insurance Daily

VENERDÌ 24 NOVEMBRE 2017 N.1238

PRIMO PIANO

Compagnie stabili in Europa

Luci e qualche ombra. Per Moody's l'outlook del settore assicurativo in Europa resta stabile. Merito soprattutto della ripresa economica e della solidità dei mercati finanziari. I rischi, tuttavia, non mancano. A cominciare da un contesto di bassi tassi di interesse che, per quanto in via di normalizzazione, pare destinato a durare ancora a lungo. Stando alle stime di Moody's, i redditi da investimento delle compagnie danni potrebbero calare fino a tre miliardi di euro entro il 2019, comportando una contrazione degli utili del 10%. Peggio ancora si prevede per le compagnie vita: il calo stimato è nell'ordine di 10-15 miliardi di euro.

Secondo Moody's, l'adattamento al contesto sfocerà in un aumento delle soluzioni unit-linked: una strategia, scrive l'agenzia di rating, che potrebbe esporre le compagnie vita a una maggior concorrenza di banche e gestori di asset. Per contro, si prevede che le compagnie danni continuino a essere molto selettive nell'assunzione dei rischi.

Resta poi la preoccupazione sulla solidità patrimoniale del settore vita in Germania: circa un terzo delle compagnie presenta infatti un *Solvency II ratio* inferiore al 100%. Permane infine il rischio geopolitico, con le incognite poste dalla Brexit e dalle tensioni nella penisola coreana. Per una news più approfondita clicca qui.

Giacomo Corvi

RICERCHE

Anche gli hacker si aggiornano

Man mano che si sviluppano e si implementano soluzioni per tutelare la sicurezza cibernetica, cambiano anche le modalità tramite cui vengono effettuati gli attacchi informatici. Kaspersky Lab individua i trend che caratterizzeranno il cyber risk nel 2018

Il *cyber risk*, con le sue numerose varianti che vanno dai furti di dati agli attacchi hacker con motivazioni politiche fino ai *ransomware*, ha dettato l'agenda del 2017. Si tratta di un tema complicato non solo perché "nuovo", ancora poco conosciuto e quindi con poche statistiche storiche, ma anche perché presenta sempre più sfaccettature, con un ampliamento continuo delle casistiche. In più, riguarda tutti i settori e le aziende di ogni dimensione, che non possono più prescindere, nell'analisi dei rischi, dal considerare le minacce derivanti dall'innovazione tecnologica. **Kaspersky Lab** ha elaborato il report *Targeted threat predictions for 2018*, in cui evidenza i possibili trend in ambito cyber security per il prossimo anno, con l'intento di fornire una panoramica che funga da bussola per le attività delle organizzazioni.

SE IL RISCHIO ARRIVA "PER VIE TRAVERSE"

Il team di ricerca monitora da diversi anni circa un centinaio di gruppi e operazioni criminali in ambito IT. Alcuni di essi sono capaci di attacchi incredibilmente sofisticati, eppure non sono rari i casi rilevati in cui, nonostante le raffinate tecnologie messe in campo e diversi ripetuti tentativi di attacco, l'intento di colpire un'azienda è andato fallito. È soprattutto il caso delle grandi imprese, che sempre più sensibili al tema della cyber sicurezza si sono dotate negli ultimi anni di potenti software di protezione e suite di difesa su misura, oltre ad aver provveduto a formare adeguatamente i propri dipendenti. Preso atto della sostanziale inattaccabilità di questi colossi, i criminali informatici hanno cercato una via alternativa, trovando una breccia nella supply chain: i fornitori, le terze parti. Attaccare le grandi imprese indirettamente, tramite aziende più piccole (e quindi verosimilmente meno protette) con cui esse collaborano, sembra essere una via efficace, come hanno dimostrato i casi di *Petya* e *ShadowPad*. È questa, secondo la ricerca, la tipologia di rischio che sarà protagonista dei prossimi mesi. "Come previsto, gli attacchi alla supply chain si sono dimostrati estremamente pericolosi" ha commentato **Juan Andrès Guerrero-Saade**, principal security researcher del team di Kaspersky Lab. "I cyber criminali – ha aggiunto – che lanciano attacchi avanzati continuano a ottenere l'accesso a società di sviluppo vulnerabili e prevediamo che lo sfruttamento dei software più celebri diventerà un vettore di attacco sempre più invitante. Gli attacchi alla supply chain permetteranno ai criminali di ottenere l'accesso a molteplici aziende in settori critici senza attirare l'attenzione di amministratori e soluzioni di sicurezza".

IL MOBILE, UNA ZONA GRIGIA

Un'altra tipologia di attacco cyber ancora poco inquadrabile è quella che riguarda le tecnologie mobile. La maggior parte dei sistemi operativi utilizzati (*Ios* fra tutti) ha sviluppato propri algoritmi di sicurezza e non permette l'installazione di software di protezione esterni. Se l'esperienza di queste multinazionali della tecnologia potrebbe costituire un fattore rassicurante, non sono poche le incertezze che derivano da una sostanziale impossibilità di controllo e intervento su quanto avviene sul proprio dispositivo. Nel caso di un'infezione, a meno che non arrivi a interferire con l'interfaccia e l'usabilità del dispositivo, è impossibile accorgersene e intervenire. Questa sorta di zona grigia costituirà terreno fertile per i malware, secondo gli esperti. *(continua a pag. 2)*

(continua da pag. 1)

NIENTE PIÙ ATTACCHI "ALLA CIECA"

I prossimi mesi saranno caratterizzati da un altro macro trend: gli attacchi *alla cieca*, generici, saranno sempre meno. Nel momento in cui la vulnerabilità dei sistemi diminuisce, perché vengono implementate misure di sicurezza, ai criminali informatici conviene infatti partire da un'analisi preventiva, un'attività di ricognizione e profilazione dell'azienda per individuarne gli asset più esposti, prima di agire. Esistono oggi dei veri e propri *toolkit* di profilazione, che sono in grado di restituire informazioni come il tipo di browser utilizzato e gli orari di maggior attività, che permettono operazioni precise e puntuali. Una problematica crescente per cui sarà necessario progettare nuovi strumenti di supervisione.

LIMITARE LE COMODITÀ DEL WWW?

Le informazioni sensibili e personali che circolano in rete sono numerosissime e distribuite su un numero difficilmente calcolabile di database, e quanto siano esposte al rischio di furto o frode lo dimostrano incidenti come il *data breach* subito dalla società di revisione contabile statunitense **Equifax**, che a luglio ha visto violati i dati di 145 milioni di americani. Molti utenti, soprattutto i nativi digitali, sembrano non essere ancora particolarmente sensibili a questo tema, mentre la preoccupazione è tangibile tra le imprese, che sono chiamate legalmente a garantire la tutela di questi patrimoni. I dati sono un pilastro per le moderne attività, si pensi ad esempio ai colossi dell'e-commerce, ma cosa succede quando la loro proliferazione raggiunge una dimensione tale da renderli difficilmente proteggibili? Sarà necessario, secondo lo studio, che istituzioni governative e società private trovino un compromesso tra le comodità derivanti dalla condivisione delle informazioni e il dovere di assicurarne la tutela.

I SETTORI PIÙ ESPOSTI

Alcuni settori rappresentano, per la loro crescente dipendenza dal mondo tecnologico, un target più esposto rispetto ad altri. Kaspersky Lab prevede che nel 2018 una delle aree più a rischio sarà quella delle imprese sanitarie. Con l'aumento del numero di attrezzature mediche specialistiche connesse alle reti informatiche, è infatti probabile una crescita degli attacchi ai network sanitari, per frodare i dati sensibili o per inficiare la funzionalità delle strutture stesse, a scopo di estorsione, interruzione del servizio o, peggio ancora, per attacchi mirati alla salute delle persone. Per quanto concerne i servizi finanziari, la crescente sicurezza dei servizi di pagamento online spingerà probabilmente i cyber criminali a prediligere gli attacchi finalizzati a ottenere il controllo degli account. Le valutazioni relative a questo settore suggeriscono che le frodi di questo tipo costeranno miliardi di dollari. Un'altra area oggetto di attenzione, e in rapidissima evoluzione, è quella delle auto connesse, che stanno delineando uno scenario inedito, in cui le minacce alla sicurezza potrebbero sorgere da fonti ancora difficilmente individuabili.

Chiara Zaccariotto

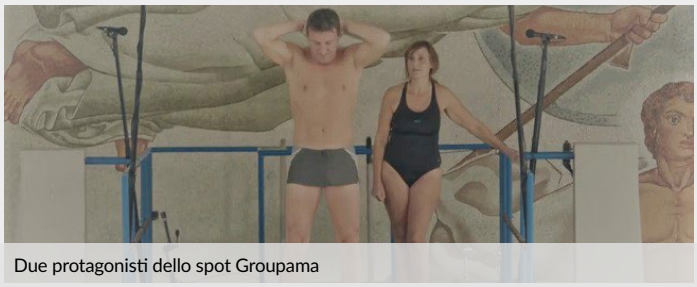
Insurance Daily

VENERDÌ 24 NOVEMBRE 2017 N.1238

MARKETING

Oltre 100 mila visualizzazioni per lo spot di Groupama Italia

Il rischio di buttarsi da un trampolino alto dieci metri anima la nuova campagna pubblicitaria per la soluzione My Protection: nasce così un video che ha tutte le caratteristiche per diventare virale



Due protagonisti dello spot Groupama

"Abbiamo chiesto a un gruppo di persone di tuffarsi da un trampolino di 10 metri". Inizia così l'esperimento sociale che **Saatchi & Saatchi,** in collaborazione con i documentaristi **Maximilien Van Aertryck** e **Axel Danielson**, ha trasformato nella nuova campagna pubblicitaria di **Groupama Italia**. L'obiettivo è raccontare la diversità di approccio al rischio di ogni singolo individuo: un gruppo di persone è stato messo di fronte alla difficile decisione di tuffarsi in piscina da un trampolino di 10 metri. Le reazioni sono buffe e divertenti. C'è la paura, il dubbio, lo sconforto di chi rinuncia e, infine, la determinazione di una tuffatrice che risponde alla sfida in modo talmente naturale che fa sembrare tutto semplice. Lo spot catalizza l'attenzione dello spettatore, che attende di vedere come persone comuni affronteranno la sfida. La strategia comunicativa di Groupama punta sulla viralità del video in rete, che sul canale YouTube *GroupamaItalia* ha già superato le 100 mila visualizzazioni. Un ottimo risultato visto che il video è stato postato il 20 novembre. La campagna pubblicitaria sarà *on air* per quattro settimane con una pianificazione multicanale che, oltre al video web, comprende due spot radio trasmessi sulle principali emittenti nazionali e locali, e una campagna di affissioni dinamiche e statiche nelle maggiori città italiane.

A.G.P.

INIZIATIVE

Innovation by Ania, si parte il 28 novembre

Al via il primo evento curato dall'associazione sul tema dell'innovazione e della mobilità. Parteciperà anche il ministro dell'Economia, Pier Carlo Padoan

Il prossimo 28 novembre a Roma, ci sarà il primo evento organizzato da **Ania** dedicato interamente all'innovazione, nell'ambito dell'osservatorio *Innovation by Ania*, appositamente creato. L'appuntamento è in collaborazione con **Deloitte,** e sarà il primo passo per "un laboratorio permanente – si legge nella nota di Ania – pensato per dare ulteriore concretezza alla modernizzazione che le compagnie di assicurazione stanno sperimentando nei propri processi e nell'elaborazione di nuove soluzioni per gli italiani".

La giornata è stata intitolata *Innovazione e mobilità: dall'auto alla sharing economy e alla smart mobility* e, oltre alla presidente dell'Ania, **Maria Bianca Farina**, parteciperà anche il ministro dell'Economia, **Pier Carlo Padoan**. Sarà presentato lo studio di Deloitte, *Innovazione e mobilità: i trend attuali e i possibili scenari futuri* .

L'osservatorio Innovation by Ania si prefigge di replicare ciclicamente per comunicare i risultati delle ricerche e degli approfondimenti sui principali temi che riguardano l'innovazione e che coinvolgono l'assicurazione e il Paese.

"L'Osservatorio – dicono dall'associazione – si concentrerà sui trend, sui profili tecnologici che li caratterizzano, sulle implicazioni normative e sulla *customer experience*. Nel primo anno saranno effettuati approfondimenti verticali sulla tematica affrontata nell'annual meeting. Negli anni successivi saranno analizzate altre tematiche ad alto contenuto innovativo, tra cui, ad esempio, IoT e big data".

F.A.

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 24 novembre di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577

Insurance Daily

VENERDÌ 24 NOVEMBRE 2017 N.1238

Insurance Connect

Milliman

WORKSHOP

IFRS 17 IN PRATICA

27 NOVEMBRE 2017

MILANO – LaGare Hotel Milano, Via G.B. Pirelli 20, 20124 – **9.30 - 13.00**

AGENDA :

9.30 – 10.00 - Welcome coffee e registrazione

10.00 – 10.30 - Gli aspetti strategici e l'impatto sul business
Ed Morgan, Milliman managing director Italy & CEE

10.30 – 11.10 - IFRS 17 in pratica, le principali sfide, il processo di transizione
Henny Verheugen, Milliman, principal

11.10 – 11.30 - Coffee break

11.30 – 12.00 - IFRS 17: Prevedibili impatti dal punto di vista di Generali
Massimo Tosoni, head of group accounting policy & reporting, Assicurazioni Generali

12.00 - 12.45 - An advanced solution to IFRS 17
Luca Cavaliere, Milliman, principal
Amritpal Khangura, Milliman LTS consulting actuary

12.45 – 13.00 - Q&A

13.00 - Chiusura lavori e pranzo a buffet

Il workshop si rivolge ad amministratori delegati, direttori generali, CFO, responsabili delle funzioni attuariali e bilancio.

Iscriviti su www.insurancetrade.it

Scarica il programma completo