Insurance Daily

MERCOLEDÌ 18 NOVEMBRE 2015 N. 820

CARGLASS
Il partner per la sicurezza.

PRIMO PIANO

Nuova governance per l'Ania

L'Ania si dota di una nuova governance. Le modifiche, che porteranno al nuovo assetto dell'associazione, sono state approvate all'unanimità dal comitato esecutivo dell'associazione, riunitosi a Milano. Nell'organigramma è confermato il numero di tre vice presidenti e prevista la trasformazione di alcuni organi associativi. "La riforma – spiega una nota dell'associazione – permetterà all'Ania di dotarsi di livelli di governo più articolati e snelli e di rispondere con maggiore tempestività ed efficacia alle sollecitazioni provenienti da un contesto economico, sociale e politico in profonda trasformazione". Il nuovo sistema prevede che l'attuale comitato esecutivo prenda il nome di consiglio direttivo, eletto direttamente dall'assemblea, e che sia composto da 31 membri (compresi il presidente e i vice presidenti); questo organo dovrà nominare, su proposta del presidente, i tre vice presidenti. L'obiettivo è consentire al presidente di proporre una squadra di governo dell'associazione più coesa. Il presidente non sarà più Aldo Minucci, il cui mandato è in scadenza a dicembre. In questi giorni si sta lavorando per arrivare a una candidatura forte da presentare all'assemblea elettiva del 15 dicembre: secondo le voci più insistenti, in pole position ci sarebbe Maria Bianca Farina, ad di Poste Vita.

B.M.

INTERMEDIARI

L'agente, tra etica e apertura

Un approccio proattivo che anticipi i cambiamenti, senza subirli. Questo l'auspicio di Erik Somaschini, vice presidente delll'Unione agenti Axa, in riferimento ai cambiamenti all'orizzonte e alle questioni irrisolte della categoria


Erik Somaschini, *vice presidente Unione agenti Axa*

La riforma dell'*Ana* non è più rimandabile. Ma va fatta sulla base di regole, che assicurino trasparenza. A ribadirlo, **Erik Somaschini**, titolare dell'agenzia **Axa** di Seregno (Mb), membro della giunta esecutiva e del consiglio direttivo nazionale di **Unapass** Rete Impresa-Agenzia, con responsabilità sui nuovi modelli distributivi, nonché vice presidente dell'**Unione agenti Axa** e responsabile del gruppo di lavoro sulla redditività delle agenzie.

In parallelo, Somaschini sottolinea l'importanza di chiudere la vertenza di **Fpa**, su cui Unapass ha mostrato apertura e disponibilità, accettando la proposta dell'**Ania**. Questioni urgenti per la categoria agenziale, verso cui il delegato Unapass invita a una maggiore proattività, necessaria per non subire il cambiamento.

Etica: termine strettamente legato, nella vostra professione, alla conoscenza. Dovrebbe essere un unicum indissolubile della professionalità di ogni intermediario che abbia consapevolezza di sè e del ruolo che riveste. La categoria ha cognizione di questo concetto?

Sinceramente, credo che solo una parte della categoria ne abbia cognizione, ma so anche che noi rappresentanti ci stiamo dando molto da fare per rilanciare il concetto, trovando grande interesse e terreno fertile fra numerosi colleghi. Indubbiamente, le condizioni economiche nelle quali versano gli agenti italiani non sono favorevoli alla definitiva affermazione di una coscienza etica, strettamente connessa allo sviluppo della tanto decantata professionalità.

Afferma il presidente Uea, Roberto Conforti, che la burocrazia nel settore è in grado di uccidere qualsiasi forma di vita intelligente. Lei trova difficoltà a gestire la sua agenzia, con tutte le miriadi di regole imposte dall'alto?

Certamente sì. Un agente, oggi, è costretto a dedicare mediamente solo il 20% del tempo lavorativo all'attività commerciale e ciò è evidentemente diventato insostenibile e va a discapito della redditività delle nostre aziende e soprattutto del servizio reso alla clientela, non permettendoci di esprimere attraverso una consulenza professionale il differenziale positivo, in termini di qualità, rispetto agli altri canali distributivi.

Avanza la vertenza di Fpa, con vistosi colpi di scena. Sna fa ricorso straordinario al Presidente della Repubblica, dichiarando illegittimi gli atti dopo che Covip ha commissariato il Fondo, richiedendone l'annullamento. Il passaggio è molto delicato. Quali previsioni riesce a immaginare?

Avendo fatto parte della delegazione Unapass durante le trattative con Ania, è un tema che sento profondamente, avendo anche vissuto le varie fasi in prima persona. Innanzitutto, non parlerei di secco rifiuto da parte di Sna, ma di un *ni*. Tutti auspicavamo, essendo paritetica la corresponsabilità, un'equa suddivisione del disavanzo fra Ania e agenti, sotto forma di contributo da un lato, e tagli proporzionali ai versamenti dall'altro. Ma, purtroppo, nel nuovo contesto multicanale, non c'è spazio per considerare le migliaia di agenti attivi che hanno contribuito, in modo determinante, a costruire il sistema assicurativo italiano, poiché oggi, spesso, la condivisione progettuale con le mandanti non va oltre una trimestrale.

(continua a pag. 2)

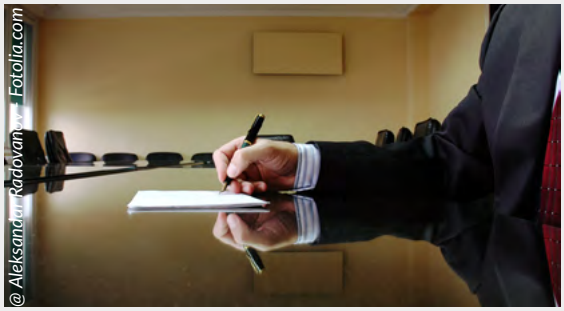
Insurance Daily

MERCOLEDÌ 18 NOVEMBRE 2015 N. 820

CARGLASS
Il partner per la sicurezza.

(continua da pag. 1)

Come Unapass, insieme ad Anapa, abbiamo deciso con grande sforzo e senso di responsabilità di accettare l'offerta di Ania, per salvaguardare l'istituzione lasciando spazio a successivi miglioramenti di primo e secondo livello. Altri hanno preferito attendere e, dopo mesi di trattative nei quali è stata data la possibilità di proporre piani alternativi, hanno deciso di scrivere alla massima carica dello Stato, cercando di delegare ad altri soggetti decisioni e relative responsabilità.



L'Ania è sempre più arroccata nel rifiutare qualsiasi soluzione che vada a migliorare la parte normativa dell'Ana, scaduto da nove anni. Sembra più propensa, assieme alle associate, a trovare accordi di secondo livello, anche su argomenti di primaria importanza. Molti gruppi aziendali respingono categoricamente questa possibilità. Il suo gruppo verso quale obiettivo tende e come interpreta il futuro dei propri iscritti?

Pensiamo che riformare e modernizzare l'Ana sia una necessità non procrastinabile, ma che le regole del gioco vadano scritte al primo livello insieme ad Ania. Questo per garantire condizioni chiare e trasparenti che consentano all'intermediario di definire liberamente il proprio modello di business (mono o pluri), in ossequio alle indicazioni dell'Antitrust che ha messo in discussione, accogliendo le istanze di alcune compagnie, questo accordo (per esempio in riferimento alla durata del mandato e al correlato importo della liquidazione). Tuttavia l'Agcm ha salvaguardato l'esistenza in generale di una piattaforma di regole base, condivise fra mandanti e agenti.

La dematerializzazione del contrassegno Rca, unita al ddl Concorrenza (in via di approvazione), può arrecare, danni alla vostra professione? Intralcia, in qualche modo, la comunicazione con il cliente? Lei cosa ne pensa di questa nuova rivoluzione?

La dematerializzazione è un passaggio ineluttabile connesso all'evoluzione tecnologica. Più in generale, ritengo che dobbiamo iniziare ad avere un approccio proattivo, teso ad anticipare, gestire e cavalcare i cambiamenti e non a subirli, come purtroppo, troppo spesso, è accaduto in passato.

Carla Barin

Insurance Daily

MERCOLEDÌ 18 NOVEMBRE 2015 N. 820

CARGLASS
Il partner per la sicurezza.

DALLE AZIENDE

Chi protegge l'identità digitale

Per mitigare i danni della guerra cibernetica, Aig ha messo a punto CyberEdge, la soluzione modulabile che tutela dalla perdita di dati personali e societari e indennizza fattispecie nuove, come il denial of service, patito da clienti e fornitori

Immaginare le conseguenze di un attacco informatico rappresenta, oggi, la prevenzione di un rischio molto concreto per ogni azienda, così come per i singoli cittadini.

La raccolta, il trattamento e la conservazione dei dati hanno assunto un'importanza fondamentale nella quotidianità: piccoli gesti di ogni giorno, all'apparenza innocui, come inviare un sms per acquistare il parcheggio o pagare l'accesso alla *Ztl*, confermare via e-mail un acquisto di forniture per i nostri uffici, rinnovare *on line* la polizze Rc auto personale o della flotta aziendale, inoltrare la dichiarazione dei redditi o pagare una bolletta, sono solo l'*input* di complessi processi informatici che comportano l'invio, il transito e la ricezione di informazioni personali, utili a identificarci univocamente e a consentirci l'accesso ai servizi, di volta in volta richiesti.

Queste informazioni così trasmesse sono la nostra cosiddetta *identità digitale*, attorno alla quale si delineano numerosi scenari di rischio: la nostra identità digitale viene rubata; la società incaricata di gestire i nostri dati e quelli dei nostri clienti, garantendone la sicurezza, non lo fa correttamente o è, suo malgrado, vittima di attacchi informatici che comportano la perdita, distruzione o sottrazione di tali dati da parte di terzi malintenzionati; un impiegato di un ente ospedaliero che, accidentalmente, rende disponibili, sul sito web dell'azienda, le cartelle cliniche e altri dati personali sensibili dei pazienti o sottrae tali informazioni minacciando di rivenderle a terzi o pubblicarle per ottenere un riscatto in denaro.

I rischi che affondano il business

Tutti possibili scenari di una guerra cibernetica, silenziosa ma in atto, le cui conseguenze sono incalcolabili: perdita di reputazione e di clienti; esposizione a richieste di risarcimento; blocco delle attività o degli impianti con conseguente perdita di profitto; ingenti costi di gestione della crisi.

Tutto questo è solo la punta di un iceberg, in grado di affondare il business di ogni azienda: nella maggior parte dei casi, i presidi aziendali di *It security* non sono sufficienti a far fronte ad attacchi strutturati e sempre più raffinati. Ecco, dunque, l'importanza di un prodotto assicurativo come *CyberEdge* di Aig, che tutela da qualsiasi perdita dei dati personali e societari, anche con riferimento a errori di trattamento commessi da *outsourcer* o dipendenti e indennizza fattispecie nuove come il *denial of service*, patito da clienti e fornitori.

CyberEdge è modulabile, copre il danno proprio da *business interruption* e fornisce innovativi *servizi pre-loss*, per assicurare l'accesso a servizi professionali utili a mitigare il danno e contenere la crisi.

RISK MANAGEMENT

Dall'attacco informatico al crimine organizzato

Gli attacchi di cybercrime rappresentano, a livello globale, più del 60% delle intrusioni in rete: un fenomeno in preoccupante crescita, come segnala l'edizione 2015 del rapporto Clusit che mostra una sorta di industrializzazione delle tecniche degli hacker

Cyber-attacco. Dietro a questa espressione può esserci di tutto. Dall'attivismo di hacker che agiscono per motivi ideologici, allo spionaggio industriale. Fino ad arrivare a una vera e propria *guerra delle informazioni*, che talvolta arriva a coinvolgere anche l'ambito militare. Diventa sempre più inquietante il quadro che emerge dall'edizione 2015 del rapporto **Clusit**, lo studio elaborato annualmente dell'associazione italiana per la sicurezza informatica.

Come ogni anno la ricerca è realizzata da un team di lavoro composto da professionisti che mettono a fattor comune le proprie competenze: quest'anno si è aggiunto il contributo della Polizia Postale e del Nucleo speciale frodi tecnologiche della Guardia di Finanza.

I dati rilevati evidenziano l'incremento del cyber crimine nei primi sei mesi del 2015: si tratta della prima causa di attacchi gravi a livello globale. Nell'ambito del cyber crimine, vanno ricondotti, il 66% degli incidenti informatici dichiarati nella prima metà di quest'anno (+6% dal dicembre 2014; questo valore era pari al 36% nel 2011), mentre gli attacchi gravi con finalità dimostrative tipici dell'*hacktivism* sono diminuiti di circa il 15% rispetto al picco del 2013. Dal 2014 rimangono sostanzialmente stabili le attività di spionaggio, mentre l'*Information warfare* (la già citata guerra delle informazioni) segna quest'anno un calo tendenziale (ma, probabilmente, per mancanza di informazioni pubbliche in merito). *(continua a pag. 4)*

@ DragonImages - Fotolia.com

Insurance Daily
MERCOLEDÌ 18 NOVEMBRE 2015 N. 820

CARGLASS
Il partner per la sicurezza.

(continua da pag. 3)

Sempre più prede nei settori Automotive e Gdo

Nei primi sei mesi 2015 i settori in cui è stato registrato il più elevato incremento di attacchi informatici sono stati quelli dell'*Automotive* e della *Gdo* (entrambi hanno visto una crescita del 400%), seguiti da *Informazione e intrattenimento* (+179%) e *Telecomunicazioni* (+125%). Un'impennata di attacchi è stata registrata inoltre, anche nelle realtà che operano nel settore *Sanitario* (+81%), così come nei *Servizi on line e cloud* (sistemi di webmail, **social media**, e-commerce), dove è stata osservata una crescita di intrusioni di oltre il 50%.

Una catena di montaggio

Lo studio mette in evidenza la tendenza all'industrializzazione delle minacce, e la completa automazione degli attacchi. Secondo gli esperti del Clusit, occorre "prepararsi all'impatto", gestendo il rischio "nell'ambito di una regia istituzionale forte". Lo scenario attuale, spiega **Andrea Zapparoli Manzoni**, membro del consiglio direttivo Clusit, "si è venuto a delineare a causa di vulnerabilità endemiche, non gestite a livello globale per troppo tempo, tanto da divenire oggi in grado di mettere realmente a rischio tutto ciò che è informatizzato. Si aggiunge la crescente capacità organizzativa dei criminali hi-tech che, indipendentemente dalla loro natura e dai loro scopi, hanno a disposizione strumenti sempre più sofisticati e relativamente economici, oltre che facilmente reperibili e completamente automatizzabili, ovvero in grado di colpire milioni di sistemi in poche ore". Secondo Zapparoli, inoltre, questo consentirebbe ai cyber-criminali di cambiare tattiche e strategie in tempo reale e di operare senza interruzione da qualsiasi punto del pianeta, traendone un vantaggio economico: per ogni dollaro investito nello sviluppo di nuovo malware, o nella ricombinazione di malware esistente per nuovi scopi, il costo sopportato dai difensori è attualmente di milioni di dollari.

Cyber-resilienza, la strategia per difendersi

Gli esperti del Clusit delineano, come unica possibilità per fronteggiare le minacce, l'adozione di una logica multidisciplinare di *cyber resilience*: "che faccia convergere compliance e cyber security, governance e risk management, cyber intelligence e crisis management, attività di prevenzione e di reazione rapida, fino alla cooperazione tra pubblico e privato e, più in generale, di condivisione delle informazioni". Secondo il Clusit, mettere in atto una politica di cyber resilience significa predisporre "un modello di rischio cyber accurato e costantemente aggiornato, che consenta di stimare le perdite potenziali al fine di determinare correttamente gli investimenti necessari in sicurezza".

L'attacco corre sul Pos

La crescente collaborazione tra gruppi cyber criminali e gruppi terroristici/paramilitari porta gli esperti del Clusit a evidenziare un possibile incremento delle logiche estorsive: organizzazioni terroristiche (come ad esempio il *gruppo Stato Islamico*) utilizzeranno sempre più frequentemente i social network per attaccare i governi. Ma anche gli stessi social continueranno a essere oggetto di attacco per mezzo di malware o frodi basate su social engineering. Inoltre, secondo lo studio Clusit, anche i sistemi Pos presentano una certa fragilità: con la diffusione di malware sviluppato ad-hoc, acquistabile a un prezzo accessibile a qualsiasi criminale comune, le singole attività commerciali potrebbero subire nel medio-breve termine attacchi. Le banche dovranno fare fronte ad una quantità maggiore di frodi e al crescente scontento degli utenti finali.

Crescerà la domanda di assicurazioni

A causa del rapido sviluppo, tutto l'universo legato all'internet of things e alle tecnologie smart e wearable connesse in rete, potrebbe essere un bersaglio immediato. A fronte dell'incremento dei rischi cyber evidenziato, gli esperti del Clusit prospettano nei prossimi mesi la diffusione della domanda di strumenti assicurativi da parte delle imprese, per le quali sarà sempre più critico operare attraverso la rete e gli strumenti informatici adottando misure correttive adeguate. La domanda, si legge nel rapporto, "sarà parzialmente frustrata dalla scarsità di offerta, e soprattutto dall'impossibilità di assicurare organizzazioni spesso prive delle più elementari misure di sicurezza (in particolare Pmi e studi professionali) per mancanza di requisiti. Si diffonderanno comunque per prime quelle polizze che offrono qualche forma di tutela legale per le vittime, e con maggiore lentezza quelle che prevedono un risarcimento dei danni subiti".

Beniamino Musto

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