Insurance Daily

LUNEDÌ 18 DICEMBRE 2017 N.1252

PRIMO PIANO

Generali cede Generali PanEurope

Generali cede la propria partecipazione in Generali PanEurope, a seguito dell'accordo firmato oggi con Life company consolidation group (Lccg). La società, che nel 2016 ha contribuito con 20 milioni di euro al risultato operativo del gruppo, opererà in qualità di partner irlandese del network Generali employee benefits.

Generali PanEurope è presente nel mercato irlandese dal 1999 e si occupa di servizi finanziari in tutta Europa per la gestione di grandi patrimoni.

Al closing dell'operazione, Generali riceverà 286 milioni, tra il corrispettivo iniziale di 230 milioni, gli interessi maturati, un possibile corrispettivo differito fino a un massimo di 10 milioni e circa 56 milioni quale rimborso di alcuni finanziamenti infragruppo. La transazione, che si chiuderà entro il primo semestre 2018, permetterà un miglioramento del Solvency II ratio di circa 0,4 punti percentuali, mentre la plusvalenza al netto delle imposte sarà pari a 56 milioni.

"Questa operazione – ha spiegato Frédéric de Courtois, group ceo global business lines & international – sottolinea il nostro impegno continuo per riequilibrare la presenza geografica di Generali nel mondo. Dopo aver avviato transazioni analoghe in altri mercati, questa operazione rappresenta un ulteriore passo avanti della nostra strategia".

Fabrizio Aurilia

INNOVAZIONE

Insurtech, un mondo a due facce

Le compagnie italiane investono ancora poco nelle nuove tecnologie. Molte le opportunità, soprattutto sul fronte della relazione con il cliente, ma anche i rischi, in particolare in tema regolamentare. Ne hanno discusso gli attori del settore assicurativo nell'evento organizzato a Roma da Ivass

L'uso sofisticato della tecnologia è un'opportunità importante, purchè la si sappia capire e cavalcare. Con questa considerazione, il presidente dell'**Ivass**, **Salvatore Rossi**, ha aperto venerdì scorso, a Roma, l'Iniziativa *Insurtech*, promossa dall'Autorità per stimolare un confronto fra imprese, intermediari, regolatori e ricercatori sull'impatto che l'innovazione ha sul mercato assicurativo, a cui norme e prassi di vigilanza devono adattarsi.

L'insurtech, ha spiegato **Rossi**, è un mondo a due facce che racchiude sia opportunità, laddove consente efficienza e riduzione dei costi, ma anche rischi, per le compagnie che non si adeguano all'evoluzione tecnologica e per il consumatore che, oggi, è esposto a nuove minacce.

Salvatore Rossi, presidente dell'Ivass

IMPRESE A RISCHIO, MA INCONSAPEVOLI

Fra i temi caldi della mattinata, quello della sicurezza informatica: area in cui il sistema produttivo italiano, investe ancora poco (4.500 euro in media, con punte di 19 mila euro per il settore Ict), nonostante il 45% delle imprese manufatturiere e dei servizi finanziari abbia subito un attacco informatico. A rilevarlo è una ricerca sul cyber risk di **Banca d'Italia**, condotta su 4 mila imprese nel periodo fra settembre 2015 e settembre 2016, secondo cui le più esposte sono le grandi realtà (62,8%), quelle ad alta tecnologia (48%) e le imprese che operano sui mercati internazionali (43%). Tuttavia, 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 è assicurato. A non spendere nulla è il 20% delle imprese, ma un 12,9% dichiara di non aver trovato una copertura adeguata.

INTERMEDIARI E CYBER RISK

Sul rischio informatico, anche l'Ivass ha effettuato, lo scorso luglio, un'indagine conoscitiva relativa su 2.900 intermediari assicurativi, da cui emerge un discreto livello di consapevolezza su questa minaccia, percepita dall'80% del campione, che ricorre a presidi di base per fronteggiare il rischio informatico. I risultati, però, ha raccontato **Maria Luisa Cavina**, responsabile del servizio vigilanza intermediari assicurativi dell'Ivass, pongono anche ombre: solo il 20% adotta policy aziendale in materia di cyber risk e test antintrusione, e solo il 22% utilizza sistemi di rilevazione accessi non autorizzati.

(continua a pag. 2)

(continua da pag. 1) Altro dato importante è quello sulla formazione specifica del personale – erogata solo dal 23% degli agenti e dal 30% dei broker – e sul ricorso allo strumento assicurativo per il rischio residuo, che coinvolge solo il 10% degli agenti, e il 12% dei broker. In sintesi, vi sono ampi margini di miglioramento e, a tal fine, l'Ivass farà una lettera al mercato per fornire agli operatori le indicazioni per una significativa mitigazione dei rischi, ripetendo poi, entro il 2019, l'indagine.

COOPERARE SUL RISCHIO INFORMATICO

Per innalzare la cyber resiliance del sistema finanziario italiano, spicca un'iniziativa di cooperazione, nata quest'anno e denominata *Certfin*, che offre servizi quali lo scambio informativo sugli eventi cyber e le nuove tecnologie usate negli attacchi per frodi e terrorismo, la valutazione degli impatti di sistema e il supporto ai singoli operatori nella risposta ai singoli incidenti. Ad oggi, all'iniziativa hanno aderito 40 soggetti e sono state gestite 830 segnalazioni degli operatori.

LA NUOVA MOBILITÀ

Altro tema caldo è quello dell'*automotive* e della *new mobility*. Secondo una ricerca internazionale di **Arthur D. Little**, intitolato *Global Automotive Mobility Study*, il 64% del campione italiano si dichiara disponibile a utilizzare l'auto a guida autonoma; il 22% la considera più sicura, ma per il 78% il problema è il *data security*.

In crescita la mobilità condivisa che, nel 2025, a livello globale, conterà 430 mila vetture, su un totale stimato di un miliardo di veicoli circolanti: aumenta l'interesse verso il *car sharing* (58% in Italia e 49% a livello globale), in presenza però di un migliore livello di servizio e un prezzo più basso. Infine, il fenomeno del *peer to peer*, ancora sconosciuto in Italia, anche se il 59% del campione nostrano si dichiara disponibile a mettere in condivisione la propria auto, nonostante preoccupi la questione normativa sulla responsabilità e l'aspetto assicurativo, ovvero la difficoltà a formulare un premio customizzato visto l'uso promiscuo.

LE OPPORTUNITÀ

Tornando all'insurtech nel suo complesso, le compagnie italiane investono in modo ancora contenuto: il 5% della quota europea che, insieme a quella statunitense, ammonta a 1-2 miliardi di euro, contro i 4-5 miliardi globali.

Tra le future applicazioni, la tecnologia di *machine learning* che offre delle promesse per l'utilizzo spinto dell'analisi sui dati, ad esempio nei claim.

In generale sono molte le opportunità che derivano dall'insurtech. Tanto per citare un caso, la possibilità di migliorare la *user experience* del cliente, fornendo servizi e coperture con logiche di *personalized insurance*: partendo dalla conoscenza dettagliata del cliente, su cui le compagnie giocano un ruolo di primo piano, si formula l'*instant insurance*.

Altro vantaggio è il basso costo della tecnologia usata in insurtech, basata su software *open source*: un'opportunità questa per l'Italia, dove la disponibilità di capitali è limitata.

I RISCHI

Tra i rischi, spicca soprattutto la cultura aziendale. In particolare, è necessario cambiare la gestione delle operation (tempi di risposta, semplicità, accessibilità e trasparenza) e il modello di relazione con il cliente, utilizzando le tecnologie per creare nuove possibilità di contatto e di servizi e far sì che l'intelligenza artificiale diventi un'opportunità per parlare di più con l'assicurato.

Altro rischio è il pricing differenziato, che rischia di fare una grossa selezione del cliente, il che fa male all'assicurato, ma anche alle compagnie che azzerano la redditività.

Inoltre, bisogna investire in capitale umano: vanno reperite risorse nuove, come i *data scientist*, ad oggi difficili da attrarre, ma anche sul piano organizzativo creando partnership con start up e *retailer*. Il tutto deve portare alla creazione di ecosistemi e relazioni industriali che, nell'allargamento della torta, possono portare a nuove revenues.

LE IMPLICAZIONI NORMATIVE

Vi è poi la questione dell'uso dei dati (il *Gdpr* è alle porte) e, più in generale, della normativa: ad oggi, le start up europee dedicano il 60% del loro tempo per la regolamentazione. In particolare, ha ricordato **Pierpaolo Marano**, docente dell'**Università Cattolica del Sacro Cuore**, la norma contempla nuove figure distributive, che svolgono attività di intermediazione senza essere iscritti o che basano la consulenza su algoritmi che non tengono conto di eventuali conflitti di interesse fra chi intermedia e il cliente, né tantomeno della normativa del Paese in cui viene utilizzato, come è il caso dei *robo advisor*. Qui mercato e vigilanza dovrebbero cooperare in un cammino di conoscenza, tenendo conto dei rischi derivanti dalle nuove tecnologie.

DIALOGO APERTO

A tirare le fila dell'intensa giornata è stato **Stefano de Polis**, segretario generale dell'Ivass che ha concluso rimarcando l'approccio dell'Autorità: stimolare l'innovazione lasciando al mercato l'iniziativa e intervenendo solo ove necessario per tutelare i consumatori. "Vogliamo sottoporre nuove iniziative e contributi di ricerca", su cyber risk, regolamentazione, utilizzo dati, educazione assicurativa, big data e proporzionalità, "mantenendo aperto il dialogo con tutti gli operatori interessati", ha annunciato.

Laura Servidio

Insurance Daily

LUNEDÌ 18 DICEMBRE 2017 N.1252

RISK MANAGEMENT

Industria alimentare italiana e responsabilità dei prodotti

Nella prima parte di questo articolo si è trattato della normativa correlata alla questione della sicurezza degli alimenti. Nella seconda parte si approfondisce il tema della difettosità di prodotto e del richiamo dello stesso secondo quanto previsto dal Codice del Consumo

(SECONDA PARTE)

In base all'articolo 117 del **Codice del Consumo**, un prodotto è difettoso quando non offre la sicurezza che ci si può legittimamente attendere, tenuto conto anche di una serie di fattori, che spaziano dal modo in cui il prodotto è stato messo in circolazione, alla sua presentazione e alle sue caratteristiche palesi, incluse le istruzioni e le avvertenze fornite.

Altri fattori determinanti sono l'uso al quale il prodotto può essere ragionevolmente destinato e i comportamenti che, in relazione ad esso, si possono ragionevolmente prevedere da parte dei suoi utilizzatori o fruitori, nonché il tempo in cui il prodotto è stato messo in circolazione.

Il difetto concepito dal Codice del Consumo ai fini della Rc Prodotti implica un'insidia o un pericolo per l'utilizzatore del prodotto e/o per i terzi che si trovano in contatto con lui. La difettosità del prodotto è generalmente riconducibile a difetto di progettazione e/o fabbricazione o all'assenza o carenza di istruzioni.

In ambito alimentare, un difetto di progettazione o fabbricazione è stato riscontrato, ad esempio, nei seguenti casi:

a) scoppio di una bottiglia d'acqua minerale nella mano di un consumatore che l'aveva presa da un bancone self- service;

b) esplosione del tappo di una bottiglia di succo verificatosi in conseguenza di procedimenti fermentativi riconducibili ad un'omessa o insufficiente pastorizzazione del prodotto;

c) presenza di un insetto all'interno di una lattina di bibita.

La definizione di "prodotto sicuro"

La giurisprudenza, al fine di identificare e valutare la sussistenza del difetto, utilizza la nozione di prodotto sicuro contenuta all'art. 103 del Codice del Consumo: "*È sicuro il prodotto che, in condizioni di uso normali o ragionevolmente prevedibili, compresa la durata e, se del caso, la messa in servizio, l'installazione e la manutenzione, non presenti alcun rischio oppure presenti unicamente rischi minimi, compatibili con l'impiego del prodotto e considerati accettabili nell'osservanza di un livello elevato di tutela della salute e della sicurezza delle persone, tenendo conto dei seguenti elementi:*

1) delle caratteristiche del prodotto, in particolare la sua composizione, il suo imballaggio, le modalità del suo assemblaggio e, se del caso, della sua installazione e manutenzione;

2) dell'effetto del prodotto su altri prodotti, qualora sia ragionevolmente prevedibile l'utilizzazione del primo con i secondi;

3) della presentazione del prodotto, della sua etichettatura, delle eventuali avvertenze e istruzioni per il suo uso e la sua eliminazione, nonché di qualsiasi altra indicazione o informazione relativa al prodotto;

4) delle categorie di consumatori che si trovano in condizione di rischio nell'utilizzazione del prodotto, in particolare dei minori e degli anziani".

Ritiro o richiamo delle merci difettose

Il Codice del Consumo contiene anche istruzioni precise circa il monitoraggio dei prodotti da parte delle autorità competenti e i requisiti che devono essere soddisfatti perché siano messi in circolazione.

Ogni prodotto può essere commercializzato solo qualora non metta in pericolo la salute e la sicurezza dei consumatori, sempreché sia usato correttamente.

Una volta che lo stesso è stato venduto, pertanto, il produttore è obbligato a controllarlo e a attuare tutte le misure necessarie per tutelare i consumatori, nel caso in cui si presentassero difetti di sicurezza.

Se il produttore non fosse in grado di agire in tal senso, le autorità competenti adotteranno misure per ordinare il richiamo di tutte le merci appartenenti alla medesima partita, anche se solo potenzialmente difettose.

Il richiamo verrà effettuato in seguito alla scoperta di difetti nella sicurezza della merce, indipendentemente dal fatto che essi dipendano dal prodotto stesso o da uno dei componenti con cui è stato assemblato. Anche la presenza di errori o carenze nelle istruzioni o nel manuale d'uso può essere sufficiente a innescare un richiamo. In ambito alimentare ciò si sostanzia generalmente in errori di etichettatura o nell'indicazione della data di scadenza.

Il rischio di immagine in un settore chiave

Oggi, la comparsa sulla stampa di avvisi sul ritiro di prodotti difettosi è sempre più comune. Il maggior numero dei richiami riguarda l'industria automobilistica, ma quasi tutti i settori sono ormai soggetti a questo fenomeno.

Le conseguenze per le imprese interessate sono notevoli: il ritiro di un prodotto può avere effetti devastanti, non solo dal punto di vista finanziario, ma anche e soprattutto sull'immagine del produttore. In particolare, il prodotto alimentare italiano vanta un livello qualitativo elevato e su questo basa la propria fortuna e popolarità in tutto il mondo.

Si pensi ai tanti ed accurati disciplinari di produzione *Dop* ed *Igp* e al geloso rispetto dei processi di lavorazione che ne garantiscono la qualità e genuinità. Alcuni prodotti sono ovunque e da sempre sinonimo del *Made in Italy*, e un colpo alla loro credibilità avrebbe effetti negativi diretti su un settore economico che vale oltre 132 miliardi di euro all'anno, oltre 30 miliardi dei quali vengono esportati.

Cinzia Altomare

(La prima parte dell'articolo è stata pubblicata su Insurance Daily di venerdì 15 dicembre. La terza e ultima parte sarà pubblicata su Insurance daily di domani martedì 19 dicembre)

Insurance Daily

LUNEDÌ 18 DICEMBRE 2017 N.1252

NORMATIVA

Polizze cyber e clausola claims made

Abbiamo pubblicato nei giorni scorsi la prima parte di questo intervento, che chiarisce vantaggi e svantaggi delle copertura "a richiesta fatta" nel rischio informatico. In questa seconda parte, si dettagliano alcune tipologie di malware che rendono più comprensibile perché i contratti loss occurence sono i meno indicati per difendersi da un attacco

(SECONDA PARTE)

Esaminiamo tecnicamente le più comuni minacce informatiche esistenti sul mercato, tenendo conto che l'abilità degli hacker (e, verosimilmente, i fondi di entità ignote e Stati nazione dietro tale business multimiliardario) consentono aggiornamenti e perfezionamenti ormai quasi giornalieri.

È notorio che un malware non necessariamente arreca danni tangibili a un computer o a un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo (*e.g. Regin malware*).

Le principali tipologie di malware sono:

Bootkit: un programma capace di insediarsi nel *boot sector* di un pc come, per esempio, l'*mbr* di Windows, non limitandosi a infettare il sistema ma, addirittura, diventando parte integrante del sistema stesso. Periodo di incubazione medio lungo.

CryptoLocker, **CTB-Locker**, **CryptoWall** e **TeslaCrypt**: sono solo alcune delle molte varianti di *crypto-malware* che vengono reimpacchettati ogni ora con lo scopo di impedirne l'intercettazione e che per questo vengono anche chiamati *malware polimorfici*, cioè mutanti. Tale caratteristica è ottenuta attraverso l'attivazione dal medesimo link, a intervalli di tempo molto ravvicinati, di file totalmente diversi. Con una frequenza di mutazione/distribuzione così assidua, i software antivirus basati su un approccio preventivo tradizionale non sono in grado di bloccare i crypto-malware, che hanno un periodo di incubazione praticamente nullo.

Ransomware: sono generalmente dei malware mutanti. La loro mutazione si ottiene attraverso l'attivazione di file totalmente diversi dal medesimo link a intervalli di tempo molto ravvicinati, anche nell'ordine del quarto d'ora. Da questi link vengono scaricati i file che potranno scatenare la crittografia dei dati o, in alternativa, l'attacco di altre tipologie di virus quali *dropper*, *rootkit* eccetera. Di fatto, con una frequenza di mutazione e distribuzione così ravvicinata, nessun software basato su un approccio preventivo tradizionale (scudo residente in tempo reale basato sulle firme di identificazione), sarà ragionevolmente in grado di bloccare preventivamente. Hanno inoltre un periodo di incubazione praticamente nullo.

L'attivazione del ransomware produce immediatamente gli effetti malevoli e dannosi come il blocco dei file di uso più comune quali Doc, Xls, Mdb, Jpg eccetera e, in più di qualche occasione, anche i file di backup di alcuni dei più comuni sistemi in uso.

Regin malware: il 24 novembre 2014 **Symantec**, la nota società che si occupa di sicurezza, ha pubblicato un rapporto sul malware *Regin*, un *trojan* protagonista di campagne massive di spionaggio realizzate ai danni di obiettivi internazionali che includono aziende, enti pubblici e istituti di ricerca.

Trojan horse: molto spesso celati sotto dei programmi che offrono utili funzionalità per indurre l'utente a utilizzarli. Non hanno capacità di replicazione, quindi devono essere inviati consapevolmente alla vittima. Contengono svariate istruzioni maligne che possono avere varie funzionalità. Possono avere periodi di incubazione brevi o lunghi a seconda del tipo di malware trasmesso.

Virus: per capire cos'è e come funziona un virus informatico dobbiamo prima capire perché si chiama in questo modo. I virus informatici prendono il nome grazie alle analogie con i virus biologici. Un virus informatico attacca determinati tipi di file modificandone totalmente o parzialmente il funzionamento permettendo anche di replicarsi, mentre un virus biologico, invece dei file, modifica le cellule per gli stessi scopi. I virus biologici hanno la capacità di rimanere silenti e quindi di non mostrare alcun sintomo (incubazione), alcuni virus informatici hanno la medesima capacità. I virus informatici non utilizzano internet per la loro diffusione, ma devono appoggiarsi per forza di cose a un programma esistente, infettandolo modificando parte del codice. Il programma infetto deve essere avviato da parte dell'utente. Essi non sono più diffusi come in passato, visto l'avvento di Internet che ha aperto strade verso le attualmente più diffuse forme di malware.

Worm: sono piccolissimi software autoreplicanti, indipendenti, capaci di infettare non solo un singolo file, ma un intero sistema operativo in modo da avviarsi autonomamente. Per la diffusione utilizzano spesso tecniche di ingegneria sociale applicata alle mail e a siti internet poco affidabili, oppure sfruttano dei bug per insediarsi all'interno di un pc senza l'ausilio di un utente esterno. Sono tra i più diffusi attualmente. Il più delle volte si limitano a rallentare il sistema operativo facendolo lavorare inutilmente. Possono avere periodi di incubazione di media durata (qualche mese).

(continua a pag. 5)

Insurance Daily

LUNEDÌ 18 DICEMBRE 2017 N.1252

(continua da pag. 4) Quasi la metà delle infezioni rilevate hanno interessato privati e piccole imprese e, in particolare, gli attacchi alle società di telecomunicazioni sembrano essere stati progettati per accedere al traffico telefonico. Si tratta di un malware complesso, difficile da rilevare, e il cui sviluppo e funzionamento hanno certamente richiesto un notevole investimento di tempo e risorse. Il malware in discorso cattura le credenziali, monitora il traffico di rete e acquisisce illegittimamente informazioni sui processi in esecuzione e utilizzo di memoria. Regin è un malware flessibile che consente agli attaccanti di eseguire azioni personalizzate in base a singoli obiettivi decisi di volta in volta. Utilizza tecnologia *Stealth* per renderlo talora invisibile anche ai più sofisticati software di contrasto. Anche quando è individuato, è spesso difficile capire cosa stia facendo e come stia operando. Symantec fu in grado soltanto di analizzare il *payload* dopo aver decriptato alcuni files campione. Ha periodi di incubazione potenzialmente lunghissimi e comunque modificabili dall'aggressore.

I vantaggio della claims made

Alla luce di tutto quanto sopra esposto, salvo poche eccezioni (Ransomware e CryptoLocker), la maggior parte dei malware in circolazione opera con periodi di incubazione lunghi o potenzialmente molto lunghi. E sono difficilmente individuabili.

Il periodo intercorrente tra l'accesso (l'*infection*) e il manifestarsi dei sintomi e dei danni è variabile, ma tendenzialmente può anche essere di alcuni mesi e in alcuni casi anche di anni. È quindi interesse dell'assicurato, più che dell'assicuratore, beneficiare di una polizza assicurativa cyber in forma *claims made* piuttosto che *loss occurrence*. Ciò considerando soprattutto la difficoltà, in moltissimi casi, di risalire alla data esatta dell'infezione, operazione che potrebbe avere costi di *forensic expert* talora elevatissimi e ben superiori ai sottolimiti di polizza. Il principio indicato dalle Sezioni Uniti della Cassazione nel 2016 e, recentissimamente, applicato dalla terza sezione civile della Cassazione, mediante richiamo ai principi di meritevolezza della tutela ex art. 1.322 secondo comma, C.C., potrebbe pertanto non applicarsi a fattispecie di rischi cibernetici, laddove la tutela opera esattamente in senso contrario.

Alberto Batini,
senior partner, Batini Traverso Grasso & Associati – Btg Legal

(La prima parte dell'articolo è stata pubblicata su Insurance Daily di venerdi 15 dicembre)

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