INSURANCE Daily

LUNEDÌ 8 MARZO 2021 N. 1907

PRIMO PIANO

Cattolica scioglie i suoi nodi

Cattolica risolve le questioni aperte. La compagnia fa pace con Banco Bpm sulla bancassurance e rimedia alle irregolarità denunciate dall'Ivass lo scorso 9 gennaio a seguito dell'indagine ispettiva, rispettando così i 60 giorni richiesti dalla vigilanza.

Per quanto riguarda la prima questione, la compagnia veronese e l'istituto bancario hanno raggiunto un accordo in base al quale, spiega una nota, "vengono superate le rispettive divergenze e sono definiti i termini e le modalità di adeguamento e di prosecuzione della partnership nel settore della bancassurance e dei relativi diritti di exit così coniugando i rispettivi interessi e tenendo conto del mutato contesto economico".

Relativamente all'indagine di Ivass, che chiedeva "una significativa discontinuità" nella governance, Cattolica ha comunicato l'invio di un piano correttivo insieme all'annuncio delle dimissioni del cda (alla prossima assemblea degli azionisti, il 13 e 14 maggio). Cattolica conferma poi la vendita sul mercato delle azioni proprie, acquisite dai soci contrari alla trasformazione da cooperativa a Spa, e la presentazione in assemblea di una proposta per allineare gli emolumenti dei consiglieri "a un benchmark di mercato". Per leggere la news completa, clicca qui.

Beniamino Musto

MERCATO

Il settore assicurativo italiano è in salute

Il comparto dei rischi ha le carte in regola per uscire dalla pandemia forte e reattivo: il ramo vita resta profittevole e quello danni ha beneficiato del calo della frequenza sinistri. Il cyber risk è ancora una minaccia silente

Il settore assicurativo italiano resiste alla crisi del Covid-19 e può trainare la ripartenza già quest'anno, nonostante le incognite legate all'uscita dalla pandemia, ma anche approfittando della grande riorganizzazione del settore bancario (ancora in corso) e della selezione che molti grandi player stanno facendo a livello internazionale.

In sintesi appare questa l'evidenza principale di **S&P Global Ratings**, che ha presentato giovedì scorso la propria visione sul settore assicurativo in Italia, durante un evento in streaming durante il quale **Taos Fudji**, director insurance ratings di S&P Global Ratings, ha illustrato nel dettaglio l'andamento dei rami vita e danni.

RAMO VITA: LE COMPAGNIE RESTANO CAUTE

Partendo dal settore vita, secondo le rilevazioni di S&P, la redditività del business resta soddisfacente, grazie a un'elevata penetrazione nel mercato. Restano le pressioni sui ritorni degli investimenti a causa di un ambiente caratterizzato da tassi d'interesse, come sappiamo, ai minimi storici. Tuttavia, è giudicato di qualità il matching tra attività-passività, grazie ai nuovi prodotti con tassi garantiti sempre più bassi.

Resta la concentrazione di titoli di Stato italiani, che potrà aumentare la volatilità e impattare sulla solvibilità, soprattutto per quelle imprese che adottano la standard formula nel calcolo dell'Scr di Solvency II.

"Le compagnie – ha spiegato Fudji – sono impegnate in un percorso di riduzione dell'investimento in Btp, ma l'esposizione in valore assoluto resta sostanzialmente stabile da cinque anni, perché legata alle gestioni separate che le compagnie non possono liquidare". La strategia è quindi quella della diversificazione soprattutto verso bond governativi di altri Paesi, obbligazioni corporate, poi fixed income e una parte di equity. "Nonostante i tassi siano bassi – ha aggiunto – non vediamo i player prendere grandi rischi per compensare il calo dei rendimenti".

(continua a pag. 2)

(continua da pag. 1)

CROLLANO I RISCATTI DELLE POLIZZE

S&P si attende una ripresa del vita del +4% nel 2021, dopo un calo simile nel 2020. Crescono molto le polizze unit-linked, che nei prossimi due anni si svilupperanno a un ritmo doppio rispetto a quelle tradizionali (ramo I +4%, ramo III +8%). Nel 2020 il lockdown ha di fatto favorito la tenuta delle polizze vita perché sono diminuiti i riscatti, che sono crollati nel 2020 ai minimi da 10 anni. Le nuove sottoscrizioni, come si diceva, presentano minimi garantiti pari o vicini allo 0%: sullo stock totale, il 50% dei contratti ha un minimo garantito allo 0%.

"Il settore – ha precisato l'economista – continua a concentrarsi anche a livello europeo, ma a differenza del mercato bancario quello assicurativo è già molto cross-border. I bassi tassi e la compressione dei margini portano i gruppi assicurativi a fare scelte radicali perché non possono permettersi investimenti digitali in tutti i Paesi in cui sono presenti. È il caso di **Aviva** – ha continuato Fudji – che sta uscendo da molti mercati che non ritiene più core per concentrarsi in altri Paesi".

Parallelamente, argomentano da S&P, il consolidamento bancario in Italia influenza le scelte delle società assicurative: la vicenda della disdetta da parte di Banco Bpm dell'accordo stipulato con Cattolica, e la conseguente recentissima risoluzione della controversia attraverso un nuovo patto (vedi Primo Piano), è paradigmatica di un settore in piena evoluzione.

RAMO DANNI: REDDITIVITÀ SOLIDA E RISPARMI PER LE COMPAGNIE

Anche nel settore danni, la redditività tecnica resta solida, anzi nel 2020 beneficia della minor frequenza sinistri, soprattutto nel *motor*, a causa del lockdown totale di marzo e aprile scorsi, delle limitazioni agli spostamenti e del turismo. In generale il non auto sta lentamente aumentando il suo peso, ma la penetrazione è ancora relativamente bassa (1,9% del Pil nel 2019 rispetto al 5,9% del settore vita).

Relativamente all'influenza della pandemia nel ramo danni, la premessa è che, a differenza di altri Paesi più coinvolti nelle questioni legate alla business interruption, il settore italiano resta relativamente immune a shock di mercato. "Solo per il business auto – rivela l'economista – stimiamo un miglioramento di sette punti percentuali del combined ratio nel 2020, quindi +3,5% meglio per tutto il settore: un risparmio notevole per le compagnie". La buona redditività del segmento auto, aggiunge Fudji, è stata agevolata anche da cambiamenti normativi, soprattutto in tema di abbassamento del costo dei sinistri.

Ma questo risparmio si è già interrotto perché, dai dati di S&P, la frequenza sinistri oggi sembra tornata già al livello pre-pandemia.

CYBER RISK: UN SETTORE ANCORA DI NICCHIA

Le varie restrizioni attuate dai governi tra la fine del 2020 e l'anno in corso, secondo S&P, non avranno conseguenze molto gravi nel biennio 2021-2022 sia per il mercato assicurativo sia per l'economia in generale: la casa americana prevede una forte ripresa già nel corso di quest'anno, con la conseguenza che la redditività diminuirà leggermente, ma potranno crescere i volumi del 2-3% all'anno. Nel mercato danni permangono tuttavia forti barriere all'ingresso, dovute all'alta concentrazione dei premi in mano a poche compagnie e ai canali di distribuzione troppo poco liberalizzati.

S&P ha dedicato al termine dell'evento anche un breve focus sul rischio cyber. Secondo quanto rilevato dall'agenzia di rating, in Italia il mercato cyber resta un settore di nicchia, la cui espansione è rallentata dal fatto che in tante polizze danni non è evidenziato se il rischio informatico è incluso o escluso: "molte aziende – ha ricordato Fudji – credono di essere coperte sul quel fronte perché il rischio non è esplicitamente escluso". Un altro fattore di rallentamento della penetrazione della copertura è la media del costo dei danni del sinistro, molto inferiore a quella, per esempio, di un incendio. Però ora la media europea si sta alzando molto: nel 2019 era di 10mila dollari per sinistro, mentre nel 2020 è stata di 60mila, con una ricorrenza molto elevata. Infine, un'azienda su cinque ha dovuto pagare un riscatto a seguito di un attacco ramsonware.

Fabrizio Aurilia

INSURANCE Daily

LUNEDÌ 8 MARZO 2021 N. 1907

RICERCHE

Per Clusit il Covid ha cambiato anche il cyber

L'annuale rapporto dell'associazione italiana per la sicurezza informatica rileva un aumento del 12% a livello globale degli attacchi. La pandemia ha incrementato le azioni di spionaggio e le aggressioni verso i dispositivi personali, mentre sono rallentate le azioni dirette verso le organizzazioni

Continua il trend di crescita degli attacchi informatici registrato negli ultimi anni e si evidenzia nel contempo una elevata capacità delle organizzazioni criminali di adattarsi rapidamente al mutare delle situazioni. Il 2020 in questo senso è stato emblematico, con l'evento pandemico che ha in parte modificato l'attività e gli obiettivi dei cyber criminali.

Nel suo annuale *Rapporto sulla sicurezza cyber*, **Clusit** ha evidenziato nel complesso un trend di crescita degli attacchi in linea con gli anni precedenti, sono invece cambiati in parte modalità e obiettivi. Lo scorso anno gli attacchi gravi rilevati a livello globale, cioè quelli che hanno un impatto sistemico che colpisce ambiti diversi, dalla politica all'economia e alla geopolitica, sono stati 1.871, una media mensile di 156 contro i 139 registrati nel 2019: il tasso di incremento annuale è del 12%, in linea con i quattro anni precedenti che segnano complessivamente un +66% rispetto al 2017. Si tratta ovviamente del numero di eventi di cui è stata data informazione e non è possibile risalire alla quantità reale e complessiva degli attacchi.

L'attività a finalità più prettamente criminale è la causa dell'81% degli attacchi gravi rilevati, mentre il 14% riguarda tentativi di spionaggio (*cyber espionage*) correlati lo scorso anno in particolare alle elezioni presidenziali negli Stati Uniti e alle attività di ricerca per i vaccini contro il Covid-19.

I numeri, ormai elevatissimi, degli attacchi, i danni perpetrati e la difficoltà a contenere il fenomeno hanno raggiunto un livello di allarme che, secondo **Andrea Zapparoli Manzoni**, membro del comitato direttivo e co-autore dell'analisi Clusit, necessita di una riflessione da parte di tutti i portatori d'interesse dell'attività digitale: "La crescita straordinaria delle minacce cyber rappresenta ormai a livello globale una tassa sull'uso dell'Ict che arriva a duplicare il valore del Pil italiano stimato nel 2020, considerando le perdite economiche dirette e quelle indirette dovute al furto di proprietà intellettuale", afferma Zapparoli in una nota che accompagna lo studio, "è urgente che siano ripensate a fondo le logiche di contrasto e mitigazione di queste minacce, e siano messe in campo le risorse necessarie a impedire che l'adozione sempre più spinta e capillare dell'Ict, di per sé auspicabile, possa trasformarsi in un boomerang sul piano geopolitico, sociale ed economico".

Il cyber si adegua alla pandemia

L'allarme di Zapparoli appare ancora più appropriato dopo quanto accaduto nei mesi della pandemia, in cui i cyber criminali hanno mostrato una notevole efficienza e rapidità di adeguamento alle nuove "opportunità". Secondo gli esperti del Clusit, il 10% degli attacchi portati a termine a partire dalla fine di gennaio 2020 è stato a tema Covid-19, dove di fronte alla complessiva incertezza del momento e facendo leva sul sentimento di insicurezza del singolo individuo poteva risultare più semplice superare le barriere degli utenti, utilizzando agganci legati ad esempio alla ricerca di dispositivi sanitari, come le mascherine. Nel solo settore della sanità, il 55% degli attacchi a tema Covid rilevati è risultato finalizzato all'estorsione di denaro, mentre nel 45% dei casi si è trattato di tentativi di spionaggio ai danni di enti di ricerca per il vaccino e di *information warfare*, guerra di informazioni.

Con lo smartworking aggirati i sistemi di sicurezza aziendali

Emblematici in questo senso i dati rilevati per il Rapporto Clusit da **Fastweb** sugli attacchi di cyber-crime in Italia durante la pandemia. Il player delle comunicazioni ha registrato nel 2020 oltre 36 milioni di eventi di sicurezza, in netta flessione rispetto all'anno precedente soprattutto dopo l'inizio del lockdown. La ragione viene collegata all'aumentato livello di protezione attivato dalle imprese e dalle organizzazioni in considerazione del ricorso al lavoro da remoto dei dipendenti, ostacolo a cui i cyber criminali hanno ovviato aumentando il numero degli attacchi verso i dispositivi utilizzati dai lavoratori, spesso meno protetti e quindi più vulnerabili a malware e virus: sono state 85mila le aggressioni a dispositivi personali, un numero doppio rispetto allo stesso periodo del 2019.

(continua a pag. 4)

INSURANCE Daily

LUNEDÌ 8 MARZO 2021 N. 1907

(continua da pag. 3)

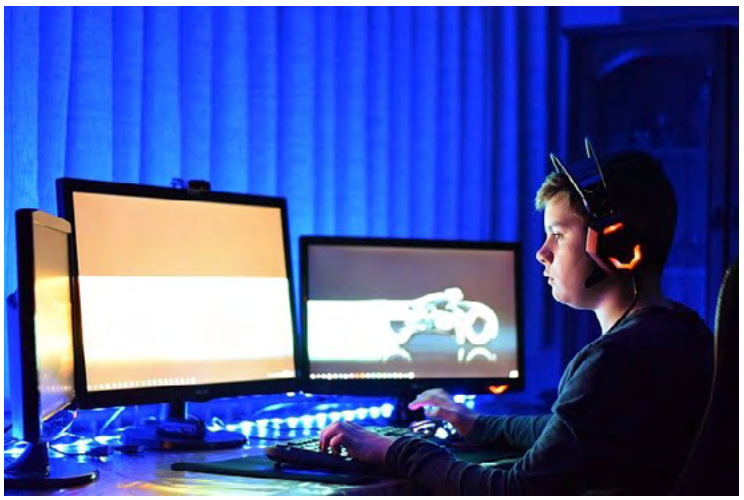
Le tecniche malware funzionano sempre

Il sistema più efficace utilizzato dalle organizzazioni del crimine informatico per portare a termini i propri intenti rimane il *malware*, in uso nel 42% degli attacchi; si tratta in prevalenza di *ransomware*, sistemi responsabili del 29% dei casi rilevati e in rapida crescita presso i pirati del web (erano il 20% nel 2019). Di rilievo anche la voce "tecniche sconosciute" (per il 20% casi di *data breach*); le tecniche di *phishing* e *social engineering* sono invece responsabili del 15% del totale degli attacchi. Clusit ha registrato, inoltre, per il 2020 un aumento del 10% degli attacchi per mezzo di vulnerabilità note, che nell'anno precedente avevano segnato una riduzione del 29%.

I settori nel mirino

Gli attacchi cyber, quando vanno a buon fine, hanno quasi sempre un impatto importante: il rapporto Clusit lo valuta come "alto" e "critico" nel 56% dei casi, nel 44% è di gravità media; anche quando si tratta di attività di *cyber espionage* la gravità è sempre più alta della media, un segnale preoccupante in considerazione del fatto che il fenomeno dello spionaggio, seppure ancora limitato rispetto a quello estorsivo e al furto che sono più prettamente conosciuti come cyber crime, è in realtà in continua crescita.

Guardando ai settori più presi di mira nel 2020, al primo posto ci sono i *multiple target* (20% del totale ma in calo del 4% rispetto al 2019), cioè gli attacchi generalizzati, su larga scala e spesso con obiettivi indifferenziati, che puntano alla logica dei grandi numeri per raccogliere il successo. Di seguito si collocano nell'interesse dei cyber criminali gli enti governativi, militari, delle Forze dell'ordine e dell'Intelligence che attirano il 14% degli attacchi a livello globale; al 12% c'è il settore sanitario, particolarmente sensibile al tema della privacy; all'11% gli enti di ricerca e dell'istruzione, subito dietro al 10% i servizi online e a seguire il *banking & finance* (8%), i produttori di tecnologie hardware e software (5%) e le infrastrutture critiche (4%).



Le rilevazioni di Clusit hanno evidenziato la crescita nell'ultimo anno degli attacchi tramite "abuso della *supply chain*", una modalità che prevede la compromissione di terze parti tramite le quali i criminali possono colpire clienti, fornitori e partner del soggetto obiettivo dell'attacco, allargando così il numero delle vittime.

Serve un intervento coordinato di sistema

L'analisi per zone geografiche elaborata da Clusit vede gli Stati Uniti come il territorio in cui si è verificata la grande maggioranza degli attacchi rilevati (47% dei casi); i paesi Europei sono stati obiettivo del 17% delle aggressioni, con una crescita del 13% rispetto al 2019; l'11% è stato rivolto a paesi asiatici mentre Oceania e Africa sembrano riscuotere tra i cyber criminali un interesse marginale (rispettivamente il 2% e l'1% degli attacchi).

Nel presentare il Rapporto, Clusit sottolinea il progressivo aggravamento della minaccia cyber per estensione e livello di aggressività, una tendenza a cui istituzioni, organizzazioni e imprese non possono essere indifferenti e che deve dare luogo a progetti di crescita tecnologica e a iniziative di sensibilizzazione e formazione verso i cittadini e in particolare i più giovani.

Maria Moro

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