INSURANCE Daily

VENERDÌ 13 NOVEMBRE 2020 N. 1845

PRIMO PIANO

Unipol, il Covid non frena l'utile

Unipol ha chiuso i primi nove mesi del 2020 con un utile netto di 759 milioni di euro, in calo del 18,5% rispetto ai 931 milioni dello stesso periodo del 2019, ma in crescita del 31,5% sui 577 milioni del risultato normalizzato, ripulito dai 421 milioni della contabilizzazione a patrimonio netto della quota in Bper e da 67 milioni di oneri straordinari per incentivazione all'esodo.

Il gruppo, tuttavia, registra una contrazione della raccolta diretta che, spiega una nota di Unipol, è stata influenzata "dagli effetti dell'emergenza sanitaria". I premi al lordo delle cessioni in riassicurazione ammontano nel periodo a 8,6 miliardi (10 miliardi al 30 settembre 2019, -13,7%).

Nel dettaglio, nel danni i premi si fermano a 5,5 miliardi (-3,6%) e calano nell'auto (-4,6%); crescono però i volumi di UniSalute, che ha incrementato il fatturato del 4,8%. Migliora significativamente il combined ratio, sceso all'86% (dal 94,1% del 30 settembre 2019). Nel vita, il gruppo ha registrato una raccolta diretta di 3,1 miliardi di euro, con un decremento del 27,2%, dovuto non solo agli effetti dell'emergenza sanitaria, "ma anche a politiche commerciali adottate con finalità di contenimento dei rischi, nonché al confronto con lo stesso periodo del 2019 caratterizzato da un elevato volume produttivo".

Beniamino Musto

RICERCHE

Il coronavirus infetta anche i computer

La pandemia di Covid-19 spinge il fenomeno del crimine informatico: nei primi sei mesi del 2020, stando all'ultimo rapporto del Clusit, si sono registrati 850 attacchi di grave entità ad hardware e reti digitali di tutto il mondo. E la stessa emergenza sanitaria sembra essere diventata un grimaldello per i professionisti del cyber crime

Il coronavirus ha finito per infettare anche i computer. La pandemia di Covid-19, soprattutto nei momenti più drammatici dell'emergenza sanitaria, ha generato quella che potrebbe essere definita la tempesta perfetta della sicurezza informatica: digitalizzazione, remote working, e-commerce, social network e persino l'inevitabile frenesia che ha caratterizzato i primi mesi di lockdown, il tutto condito dall'ancora scarsa attenzione riservata alla sicurezza informatica da cittadini, imprese e istituzioni, hanno di fatto creato le condizioni ideali per sostenere l'attività dei criminali del web. Il risultato è che nei primi sei mesi dell'anno, stando all'ultimo rapporto del **Clusit**, si sono registrati 850 attacchi di grave entità a computer e reti digitali di tutto il mondo. Calcolatrice alla mano, fanno quasi 142 episodi al mese contro i 139 che si erano registrati mediamente nel 2019, ossia in quello che l'associazione italiana per la sicurezza informatica aveva definito nel suo precedente rapporto "l'anno peggiore di sempre" in termini di cyber risk.

"L'analisi degli attacchi nel primo semestre del 2020 rende evidente che, oggi come non mai, la nostra civiltà digitale è esposta a rischi importanti e potenzialmente sistemici", ha commentato **Andrea Zapparoli Manzoni**, uno degli autori del rapporto. "Nell'emergenza mondiale che stiamo attraversando – ha aggiunto – la cyber security è chiaramente, e in maniera irreversibile, un requisito fondamentale per il benessere di singoli individui, istituzioni ed imprese".

(continua a pag. 2)

INSURANCE Daily

● VENERDÌ 13 NOVEMBRE 2020 N. 1845

(continua da pag. 1)

UN NUOVO MONDO

Se il 2017, per usare la stessa definizione del Clusit, era stato *l'anno del salto quantico della sicurezza informatica*, ora quel grande balzo è stato compiuto e ci troviamo in un mondo del tutto nuovo. Il rapporto recupera a tal proposito la locuzione latina *hic sunt leones* per descrivere tutta la novità della dimensione in cui siamo approdati con il coronavirus. Una dimensione popolata non da mostri e chimere come pensavano i latini, e neppure dai semplici hacker a cui eravamo abituati, ma da decine e decine, come si legge nel rapporto, di "gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, Stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e contractors, gruppi state-sponsored civili e/o paramilitari e unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i server, i client, i device mobili, gli oggetti IoT, le piattaforme social e di instant messaging (e la mente dei loro utenti), su scala globale, 365 giorni all'anno, 24 ore al giorno".

Ecco perché, se il crimine informatico evolve, anche le contromisure devono andare nella stessa direzione. "Il digitale sta trasformando l'organizzazione delle imprese e la vita dei cittadini, e stiamo comprendendo che la sicurezza del digitale è essenziale", ha osservato **Gabriele Faggioli**, presidente del Clusit. "Pensiamo – ha proseguito – che siano tre in particolare i punti da indirizzare nel percorso virtuoso verso la sicurezza informatica: investire in ricerca e innovazione, costituire un ecosistema delle imprese e della pubblica amministrazione in cui gli investimenti risultino adeguati alla minaccia e consapevolizzare maggiormente i cittadini".

IL GRIMALDELLO DELLA PANDEMIA

L'evoluzione del cyber risk è diventata immediatamente evidente con la pandemia di coronavirus: in appena sei mesi, i professionisti del crimine informatico sono riusciti a trasformare l'emergenza sanitaria in un grimaldello per accedere ai computer e ai dati degli utenti. Secondo i numeri del rapporto, ben 119 episodi, pari al 14% del totale, possono essere riferiti a strumenti o tecniche legati al Covid-19.

La maggior parte degli attacchi collegati al coronavirus sono stati realizzati nell'ambito del *cyber crime* (72%), ma anche settori come *espionage/sabotage* (24%) e *information warfare* (4%) hanno saputo trarre vantaggio dalla situazione. Gli autori di queste incursioni hanno fatto ricorso principalmente a *phising/social engineering* (61%) e *malware* (21%), tecniche utilizzate soprattutto all'interno di attacchi diretti a molteplici obiettivi (64%) e pertanto finalizzati a colpire e danneggiare contemporaneamente il maggior numero possibile di persone e organizzazioni. Il coronavirus si è inoltre rivelato spesso il vero protagonista dell'attacco. Il rapporto, a tal proposito, cita alcuni casi di *bec scam*, una tecnica di intrusione informatica che consiste nel prendere possesso dell'account di posta elettronica di un responsabile aziendale e nel convincere fraudolentemente, attraverso una o più e-mail, un ignaro dipendente a trasmettere informazioni riservate dell'impresa: questa tipologia di attacco, stando al rapporto, è stata utilizzata soprattutto nelle prime fasi della pandemia, sfruttando la frenesia generata dalla difficoltà di rifornirsi di dispositivi di protezione individuale come le mascherine.

TUTTI SONO UN BERSAGLIO

Il cyber risk non è tuttavia un'altra novità portata dal coronavirus. Il rischio informatico esiste da tempo. E la pandemia di Covid-19 ha soltanto aggravato una situazione resa già precaria dall'ancora scarsa attenzione riservata alla pratica della sicurezza informatica.

Tutti oggi (ma anche ieri) sono esposti al rischio. Basti pensare che la maggioranza degli attacchi complessivi è ancora diretta a obiettivi multipli (25%), seguita da istituzioni governative e militari (14%), servizi online e cloud (10%), strutture sanitarie (10%) e istituti formativi e di ricerca (10%). Anche la distribuzione geografica degli attacchi fa ben comprendere come la minaccia sia ormai globale. Quasi la metà degli episodi (45%) ha colpito obiettivi situati in Nord America, ma è significativa la crescita registrata in Europa: nel giro di un anno, la quota di attacchi avvenuti nel vecchio continente è passata dal 9% del primo semestre del 2019 all'attuale 15%. A dimostrazione del fatto che il cyber risk (se mai lo fosse stato) non è più un fenomeno circoscritto a determinati settori o aree geografiche. E che tutti, purtroppo, sono un bersaglio.

Giacomo Corvi

INSURANCE Daily

VENERDÌ 13 NOVEMBRE 2020 N. 1845

PRODOTTI

Axa XL lancia Risk scanning

La soluzione consente ai risk manager di generare valutazioni delle proprie sedi aziendali per area, Paese e rischio, così da comprendere meglio le specifiche esposizioni e adottare interventi mirati per la gestione e il trasferimento del rischio

© Sergey Nivens - Fotolia

Axa XL Risk Consulting ha annunciato il lancio di un nuovo servizio di valutazione dei rischi: *Risk scanning*. Disponibile su scala globale, questa soluzione è stata ideata per associare l'esperienza dei consulenti del rischio di **Axa XL** con le capacità di data mining e gli algoritmi probabilistici, per eseguire valutazioni multirischio delle varie sedi di un'azienda.

Risk scanning consente ai risk manager di generare valutazioni delle proprie sedi aziendali per area, Paese e rischio, così da comprendere meglio le specifiche esposizioni e adottare interventi mirati per la gestione e il trasferimento del rischio.

Secondo **Maxime Ambourg**, risk consulting manager for innovation & business development presso Axa XL Risk Consulting, i programmi tradizionali di loss prevention "solitamente sono focalizzati sulle sedi principali di un'azienda. Possono quindi sottovalutare i rischi associati alle sedi secondarie, raramente soggette alle visite dei risk engineer nonostante i sinistri si verifichino con maggiore frequenza proprio in queste sedi. Sfruttando sia l'esperienza dei nostri consulenti sia le nuove tecnologie, Risk scanning consente una valutazione più completa e, quindi, più puntuale".

Il lancio di questo prodotto, ha spiegato **Jonathan Salter**, head of risk consulting presso Axa XL, "si inserisce in una strategia più ampia, che ambisce a una ulteriore digitalizzazione della nostra offerta e a fornire un servizio migliore ai risk manager. Lo scorso anno abbiamo lanciato una suite di servizi digitali per aiutare i nostri clienti a comprendere meglio la propria esposizione alle calamità naturali e, di recente, per valutare costantemente la prevenzione delle perdite a fronte delle restrizioni legate al Covid-19".

B.M.

COMPAGNIE

Zurich archivia un buon terzo trimestre

I risultati del gruppo svizzero nei primi nove mesi del 2020 mostrano una crescita dei premi lordi, in particolare nel commercial business

Nei primi nove mesi del 2020 il gruppo **Zurich** ha registrato (a cambi costanti) una crescita dei premi lordi sottoscritti nel ramo danni, con un forte aumento del commercial insurance e un ulteriore miglioramento dei tassi. Il gruppo, inoltre, registra una ripresa delle vendite della nuova produzione vita nel terzo trimestre, con Ape in crescita del 7% a cambi costanti. Da inizio anno, tuttavia, le vendite Ape sono diminuite dell'8% a cambi costanti. Risultano in calo, invece, i premi lordi sottoscritti di **Farmers Exchanges**, la cui diminuzione è del 3%.

Il gruppo svizzero, ad ogni modo, mostra una posizione patrimoniale solida, con l'indice *Z-Ecm* stimato pari al 110% al 30 settembre 2020, e uno *Swiss Solvency Test ratio* pari al 193% al 30 settembre 2020.

Per quanto riguarda i sinistri relativi alla pandemia di Covid-19, al netto della riduzione della frequenza dei sinistri, sono rimasti invariati a circa 450 milioni di dollari al 30 settembre 2020. Le priorità per il gruppo rimangono, come spiega una nota, "il supporto ai clienti e il benessere dei colleghi in un contesto difficile per motivi di salute pubblica ed economici, e l'esecuzione della strategia incentrata sul cliente".

Secondo **George Quinn**, group chief financial officer di Zurich, nel corso del terzo trimestre, "il gruppo ha continuato a gestire con successo le sfide senza precedenti poste dal Covid-19, la recessione globale e un numero record di uragani che si sono abbattuti sugli Stati Uniti. La nostra priorità rimane il supporto ai nostri clienti e la sicurezza e il benessere dei nostri colleghi, mentre continuiamo a implementare la nostra strategia incentrata sul cliente. La crescita della nostra divisione commercial è rimasta solida, con un ulteriore miglioramento dei prezzi e delle performance. Il nostro business vita ha visto un ritorno alla crescita nel terzo trimestre, nonostante le continue sfide per i canali fisici di distribuzione, mentre Farmers ha proseguito nella sua strategia per migliorare la crescita. Nel corso dei nove mesi – conclude Quinn – il gruppo ha continuato a dimostrare la sua capacità di resilienza e solidità finanziaria, con un miglioramento della posizione patrimoniale rilevata dall'indice Z-Ecm nel corso del trimestre".

B.M.

INSURANCE Daily

● VENERDÌ 13 NOVEMBRE 2020 N. 1845

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