

PRIMO PIANO

L'anno del cyber crime

Il 2017 si è distinto per un aumento esponenziale degli attacchi hacker a siti istituzionali e di interesse pubblico, infrastrutture da cui dipende il buon funzionamento del sistema-Paese. Sono state più di mille le violazioni nel corso dell'anno appena passato. Ma le denunce che arrivano alla polizia postale e al Cnaipic, il Centro nazionale anticrimine per la protezione delle infrastrutture critiche, sono state molte di più: ben 28.522, cioè un numero cinque volte maggiore rispetto alle segnalazioni del 2016.

Le Autorità hanno aperto 68 indagini, che hanno portato alla denuncia di 33 persone e all'arresto di due individui, accusati di spionaggio informatico politico, istituzionale e industriale.

Non è un caso quindi che le segnalazioni dell'Ivass sui siti fraudolenti che commercializzano polizze siano sempre maggiori: ciò che fino a pochi anni fa si poteva fare solo fisicamente, o al telefono, oggi attraverso internet è diventato tremendamente più semplice.

Proprio ieri l'Istituto ha segnalato la promozione di polizze Rc auto tramite il sito www.europeaassicurazioni.it, che ha rubato il numero di iscrizione al Rui di un intermediario, regolarmente registrato, e ignaro di tutta la vicenda. A seguito delle verifiche del caso, l'Ivass ha chiesto alle Autorità competenti l'oscuramento del sito.

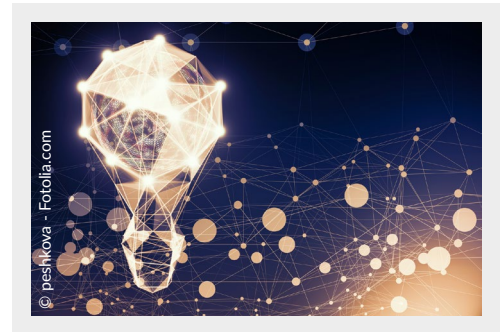
F. A.

RISK MANAGEMENT

Le strategie dell'Ocse contro il cyber risk

Puntare sull'esperienza del settore assicurativo, sulle informazioni degli enti governativi e sulla collaborazione tra questi due mondi: è la strategia dell'organizzazione, descritta nel report "Enhancing the role of insurance in cyber risk management", per contrastare il rischio digital

La trasformazione digitale sta creando per le attività economiche significative opportunità di innovazione, efficientamento dei processi e dei costi, ma questa crescente dipendenza dalle tecnologie porta con sé anche l'ampio universo dei *cyber risk*, potenzialmente distruttivo perché privo per sua natura di confini concreti. Un recente report dell'Ocse intitolato *Enhancing the role of insurance in cyber risk management* esamina il ruolo che il nascente mercato assicurativo dedicato al *digital* potrebbe rivestire nel potenziare la resilienza informatica, configurandosi come un vero e proprio partner di business per le imprese. Il documento rientra nel più ampio progetto *Going Digital*, lanciato dall'organizzazione per la cooperazione e lo sviluppo economico poco più di un anno fa (il 12 gennaio 2017) e nato con l'obiettivo di fornire ai responsabili politici e alle autorità regolatrici dei vari Paesi strumenti che aiutino le società a orientarsi in un ambiente sempre più *datacratico* e basato sul digitale.



IL RUOLO STRATEGICO DEL SETTORE ASSICURATIVO

Secondo l'Ocse, nell'ambito della sicurezza informatica ci sono diverse ragioni per ritenere il settore dell'insurance un partner strategico. A partire dalla fase di analisi del rischio: le competenze acquisite nel tempo negli altri campi, tra cui la capacità di creare sistemi di raccolta, organizzazione e interpretazione delle informazioni, consentono di quantificare l'esposizione al rischio in modo analitico e puntuale, tenendo conto dei molteplici fattori che intervengono. Si tratta di un procedimento che richiede un *know how* di ampio raggio, che include la capacità di interpretare dati ma anche quella di saper cogliere le specificità del business di un'impresa, così come il contesto in cui essa opera. Competenze che il settore assicurativo ha avuto modo di sviluppare negli anni e che, con opportuni aggiornamenti, possono rivelarsi strategiche nel campo del digitale. Lo stesso discorso vale per la definizione delle attività di prevenzione, e successivamente di gestione, del rischio. Intorno a compagnie, broker e agenti, gravita poi una rete di società che fornisce una serie di servizi che si potrebbero definire *accessori* rispetto al core business degli assicuratori, la polizza in sé, ma che sono cruciali nel momento in cui il rischio si concretizza.

(continua a pag. 2)

INSURANCE REVIEW su TWITTER
Seguici cliccando qui



(continua da pag. 1)

Dalla gestione del sinistro nell'immediato alla fase di *disaster recovery*, dal mantenimento della *business continuity* alla scelta del supporto nel *crisis management*: non considerare questi elementi può essere decisivo quanto scegliere un fornitore non adeguato. Il settore assicurativo può giocare anche qui un ruolo chiave, facilitando l'accesso a questi servizi e supportando le imprese nella loro scelta, avvalendosi di una rete e di conoscenze approfondite negli anni.

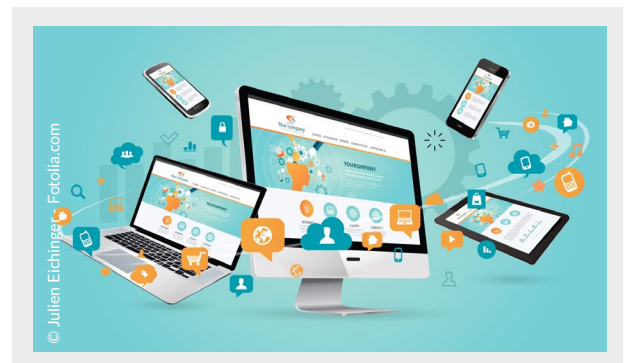
DOVE FARE UNO SFORZO IN PIÙ

Tramite l'assicurazione il rischio a carico dell'impresa viene trasferito, parzialmente o completamente, alla compagnia. Fin qui la teoria, ma la pratica si rivela spesso più complicata: secondo l'Ocse, in molti casi c'è troppa poca chiarezza su quali sono le polizze cyber disponibili sul mercato e su cosa esattamente è incluso nelle coperture. Le differenze nella terminologia e gli approcci divergenti, per cui il rischio digitale – analizzando l'offerta attuale – quando non è assicurabile a sé stante può rientrare praticamente in qualsiasi ramo assicurativo (come estensione), non aiutano la chiarezza. Sono tutti elementi che rischiano di aggravare il clima di incomprensione tra assicuratori e assicurati, che non riescono a orientarsi e non trovano chiarezza nell'offerta sul mercato. Lavorare a una terminologia e a una classificazione comune potrebbe essere, secondo l'Ocse, una scelta virtuosa che diminuirebbe l'incertezza, inevitabile nel momento in cui il mercato si deve confrontare con un rischio nuovo e mutevole come quello cyber, ma almeno in parte mitigabile.



LA COLLABORAZIONE CON GLI ENTI GOVERNATIVI

Il settore assicurativo non è il solo a cui l'Ocse chiede maggiore collaborazione. Il quadro politico, quello normativo e giuridico dei vari Paesi rivestono un ruolo fondamentale: dipendendo in gran parte da loro la quantità e la tipologia di informazioni sugli incidenti informativi diffondibili e quindi disponibili, da loro dipende inevitabilmente l'accuratezza delle analisi su cui si basa il processo assicurativo e di pricing. Più informazioni sono disponibili, più semplice è elaborare modelli e proposte di trasferimento del rischio aderenti alla realtà del mercato, e quindi convenienti sia per le imprese sia per i player assicurativi. Gli obblighi di divulgazione e notifica contenuti nel nuovo *Gdpr* vanno in questa direzione. L'obiettivo a lungo termine è quello di arrivare a istituire veri e propri archivi di segnalazione degli incidenti, che censiscano anche gli attacchi alla sicurezza delle infrastrutture governative. È una lunga strada, da iniziare a piccoli passi, il primo dei quali, secondo l'Ocse, è una maggiore collaborazione tra pubblico e privato nella condivisione delle informazioni. C'è un altro fattore di cui sia i governi sia le imprese assicuratrici dovrebbero tenere conto: gli incidenti cyber che si sono verificati fino ad oggi sono rimasti, per quanto estesi globalmente, all'interno delle capacità di gestione delle compagnie. È più che concreta però la possibilità che, per il fenomeno di accumulazione del rischio, si verifichino attacchi dalle conseguenze ben più catastrofiche, tali da non poter essere più gestiti senza un sistema di collaborazione tra pubblico e privato. È la preoccupazione che porta oggi molti player assicurativi ad applicare varie esclusioni di copertura e a limitare la propria esposizione. Il report dell'Ocse invita il settore pubblico e quello privato a collaborare per affrontare gli accumuli di rischio prima che si concretizzino, attuando congiuntamente strategie di finanziamento del rischio e di mitigazione.



Chiara Zaccariotto



INSURANCE CONNECT su FACEBOOK

Seguici sulla pagina cliccando qui 

MERCATO

Welfare aziendale, ora c'è un'associazione

È appena nata, si chiama WelfareImpresa e fa parte di Confindustria Federvarie. Ha l'obiettivo di diventare il punto di riferimento per il comparto

Dieci aziende iscritte a Confindustria Federvarie hanno dato vita a una nuova associazione tra imprese che operano nell'ambito del welfare aziendale. Si chiama WelfareImpresa e ha l'obiettivo di diventare il punto di riferimento per tutte le realtà che operano nel settore dei servizi di benefit, comparto in crescita e agevolato anche da importanti iniziative governative degli ultimi anni.

L'associazione al momento comprende Welfare Company, Poste Welfare Servizi, UniSalute Servizi, QUI! Group, Repas, Più Buono, Assiteca, Pulsar Risk e Olimpia Agency: un panorama variegato, che va da aziende specializzate a compagnie assicurative, passando per gli intermediari. Chiara Fogliani, ceo di Welfare Company è stata eletta presidente.

Le finalità principali di WelfareImpresa sono essenzialmente di due tipi. La prima di carattere divulgativo, che si attuerà attraverso la diffusione di studi e di ricerche e l'erogazione di attività di formazione, per aumentare la conoscenza del welfare aziendale e delle sue buone pratiche all'interno del sistema socio-economico, in particolare verso le imprese di piccole e medie dimensioni. La seconda attività dell'associazione sarà quella di sensibilizzare costantemente il legislatore e l'opinione pubblica sull'urgenza del completamento organico delle riforme e della razionalizzazione della normativa vigente, anche al fine di ridisegnare il sistema delle esenzioni fiscali in un'ottica più integrata.

WelfareImpresa nasce dal lavoro, iniziato nel 2011, di alcune società che emettono buoni pasto e voucher che avevano costituito il Cobes. "Promuovere la cultura del welfare aziendale - ha detto la presidente - significa per noi far comprendere a tutti che i piani di welfare sono una straordinaria opportunità di crescita economica, a tutela delle più moderne politiche di conciliazione vita-lavoro. Con le ultime leggi di Stabilità - ha continuato - sono stati compiuti significativi passi in avanti sul tema, ma ci attende una stagione di approfondimento e sistematizzazione di uno scenario vitale per il futuro del mercato del lavoro, non ultimo per il pubblico impiego. WelfareImpresa desidera dare un contributo autorevole a questo importante processo perché parlare di welfare equivale a parlare di crescita e sostenibilità del Paese".

F. A.

INTERMEDIARI

Anapa firma il nuovo Ccnl dei dipendenti di agenzia

Intesa siglata con Fisac, First, Fna e Uilca, resterà valida fino al 30 giugno 2020



Il momento della firma

È stato definito il nuovo contratto collettivo nazionale dei dipendenti di agenzia sottoscritto tra Anapa Rete ImpresAgenzia assistita da Confcommercio, e le sigle sindacali Fisac Cgil, First Cisl, Fna e Uilca. L'accordo, firmato ieri a Bologna, dopo una trattativa durata 15 mesi, sarà depositato presso il ministero del Lavoro. Il nuovo contratto, che ha durata pari a quattro anni e sei mesi (dal 1° gennaio 2016 al 30 giugno 2020) introduce "molti elementi moderni, alla luce dell'evoluzione che sta interessando il mercato assicurativo", spiega una nota di Anapa. In particolare, le novità riguardano la flessibilità dell'orario di lavoro, la possibilità per otto settimane di svolgere la prestazione lavorativa nella giornata di sabato, una diversa modulazione degli scatti di anzianità per i nuovi assunti; il passaggio da retribuzione annua a retribuzione mensile, che non rappresenta solo una modifica teorica, ma ha ripercussioni pratiche sull'attività in generale, ad esempio nell'adeguamento del criterio di calcolo del lavoro straordinario, comportante una sostanziale diminuzione degli oneri a carico del titolare.

Anapa sottolinea il fatto che, rispetto ai precedenti accordi, per quello appena siglato non è prevista una qualsiasi somma una tantum per coprire il periodo arretrato, in cui il contratto non è stato rinnovato: la quota di aumento, estremamente contenuta, si concretizza in 35 euro lordi mensili per l'intera durata. "Le parti - scrive l'associazione - hanno condiviso l'importanza di valorizzare e razionalizzare l'attività svolta dall'ente bilaterale Ebas attraverso la sottoscrizione di un accordo sulla governance della bilateralità, con l'obiettivo di rilanciare l'azione di quest'ultimo, e introducendo importanti strumenti di welfare sia per i lavoratori che per le agenzie".

Secondo il presidente di Anapa, Vincenzo Cirasola, "la sottoscrizione di questo secondo contratto collettivo è la dimostrazione che la nostra associazione è un interlocutore serio e riconosciuto a livello istituzionale e nazionale, e che rispetta i dipendenti amministrativi, asset fondamentale delle nostre imprese agenzie, offrendogli uno strumento di contrattazione moderno, in grado di rispondere alle attuali richieste del mercato del lavoro e di quello assicurativo e che certamente andrà sviluppato in futuro".

Beniamino Musto

RICERCHE

Pagamenti digitali, con Psd2 cambia tutto

È entrata in vigore (con gradualità) la normativa europea che riguarda soprattutto il settore del credito: rafforzata la sicurezza e la trasparenza delle transazioni

Il 13 gennaio è entrata in vigore negli Stati membri dell'Unione Europea della nuova direttiva sui pagamenti elettronici (*Payment services directive 2, Psd2*): un nuovo impianto normativo per i pagamenti digitali che ha lo scopo di stimolare l'innovazione e la trasparenza, rafforzando anche la sicurezza delle transazioni su internet e l'accesso di operatori terzi ai conti correnti bancari. La riforma sarà attuata in vari step e ci vorranno 18 mesi perché vada a regime.

Secondo uno studio di **Finextra**, appena pubblicato per conto di **CA Technologies**, solo il 50% delle banche italiane ritiene di riuscire a ottemperare ai requisiti minimi della direttiva entro i tempi previsti. Nonostante questo, ben il 96% dichiara di essere molto o abbastanza d'accordo sul fatto che la normativa costituirà un'opportunità per innovare, differenziarsi e creare nuovi prodotti e servizi. È un dato in parte sorprendente, perché si piazza 10 punti percentuali sopra la media degli altri 13 Paesi europei in cui è stata effettuata la ricerca.

"Anche se molte banche italiane – si legge nella ricerca – hanno in progetto di limitarsi in prima istanza a soddisfare i requisiti minimi della Psd2, esse partono dal presupposto che, nel lungo periodo, tale normativa sarà foriera di nuove aperture e innovazioni".

Un cambiamento a lungo termine

La ricerca mostra come gli istituti italiani considerino la nuova normativa come un fattore strategico per il cambiamento a lungo termine: solo il 21% delle banche la riduce a obbligo normativo. Questa tendenza è confermata nel 92% dei casi, dove la *digital transformation* è responsabile, o comunque coinvolta, nell'attuazione della Psd2. Per le banche, quindi, l'innovazione nel settore dei pagamenti è parte integrante della strategia digitale.

Secondo quanto rivelato dalla ricerca di Finextra, la tecnologia è la chiave per il successo in questo campo: l'83% delle banche italiane è molto o abbastanza convinto di dover acquisire nuove tecnologie per l'attuazione completa di Psd2 e dell'*open banking*, cioè la condivisione dei dati bancari (in modo sicuro) con terze parti. Il 21% degli intervistati si è espresso a favore della creazione di ecosistemi orientati ai clienti insieme ai partner fintech.

Tuttavia, restano ancora molte criticità. Il 79% degli istituti italiani pensa che la mancanza di competenze specifiche, i vincoli di budget, i problemi tecnologici, la presenza di sistemi legacy e i rischi legati alla sicurezza siano i problemi ancora aperti cui mettere mano.



La metà delle banche italiane intervistate, cioè 13% in più della media europea e 24% sopra il dato relativo alla Francia, ritiene che la clientela nostrana non sia pronta per l'open banking: ciò spiega anche perché il 78% delle banche sia pronto a un periodo minimo di due anni per rientrare dai relativi investimenti.

Verso l'era dell'open banking

Nell'era *post-Psd2*, i competitor delle banche saranno i soliti noti: **Google, Amazon, Facebook e Apple**. Ma, secondo la maggioranza delle banche, la sfida lanciata da giganti dell'hi-tech, nel breve termine, non costituirà un pericolo diretto.

Poco più di un quarto delle banche italiane crede che la principale minaccia sarà la competizione interna al settore da parte dei player tradizionali, i cui punti di forza sarebbero proprio la gestione delle relazioni con la clientela e il possesso dei dati. Circa il 14% teme invece le nuove banche online che si troverebbero di fatto nella posizione ideale per cavalcare le opportunità della direttiva, essendo più agili e non vincolate dalle legacy.

"Per sfruttare questa nuova opportunità – dicono gli analisti – le banche italiane devono svecchiare le proprie architetture applicative, stringere nuove partnership collaborative, accelerare l'open banking (nonostante le perplessità, ndr) e introdurre innovazioni più snelle nei pagamenti digitali, a prescindere dal proprio stadio di maturità rispetto alla direttiva Psd2".

Fabrizio Aurilia

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