INSURANCE Daily

LUNEDÌ 13 GIUGNO 2022 N. 2181

PRIMO PIANO

Cesare Lai passa ad Howden

Cesare Lai entra in Howden come head of employee benefits and wellbeing in Italia. "Sono fiero di entrare a far parte di questo progetto straordinario in Howden, in un momento così cruciale per il settore", ha commentato Lai. "Le aziende richiedono consulenti qualificati e soluzioni tecniche innovative per offrire la migliore esperienza possibile ai loro dipendenti e poter continuare ad attrarre e trattenere talenti: non vedo l'ora – ha aggiunto – di lavorare con i clienti in Italia e fornire loro le migliori soluzioni per adattarsi a queste nuove esigenze". Lai vanta una lunga esperienza in società come Aig, Mercer e Willis Towers Watson: recentemente aveva ricoperto l'incarico di ad di Generali Welion. La nomina, ha detto Glenn Thomas, global practice leader di Howden per gli employee benefits, "rafforza il nostro impegno nel servire clienti con esigenze multinazionali e conferma il nostro obiettivo di attrarre i migliori talenti e accrescere la nostra presenza internazionale.

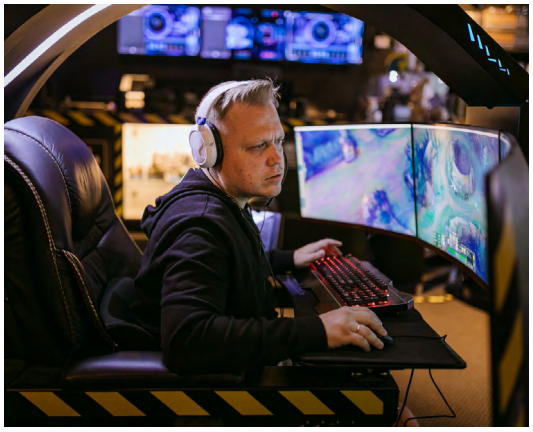
Il gruppo ha anche annunciato l'acquisizione di TigerRisk Partners, società di brokeraggio specializzata nella riassicurazione e nella consulenza strategica. L'operazione avverrà a un prezzo complessivo di 1,6 miliardi di dollari.

Giacomo Corvi

RISK MANAGEMENT

Attacchi DDoS e strategia per la sicurezza nazionale

In seguito all'invasione dell'Ucraina e alla cyberwar che ne è derivata in tutto il mondo, le nostre infrastrutture sono sotto attacco da parte degli hacker di entrambi gli schieramenti. Ecco quali sono le iniziative del governo per metterle in sicurezza e garantire i servizi forniti a milioni di utenti in tutto il Paese



Lo scorso 17 maggio, il **Csirt** (acronimo di Computer security incident response team), ovvero l'istituito creato nel 2018 presso l'**Agenzia per la cybersicurezza nazionale** con l'intento di monitorare eventuali incidenti sul nostro territorio, ha emanato un bollettino sulle attività di preparazione di attacchi *DDoS* verso le nostre infrastrutture.

Il DDoS (Distribuited denial of service) è un attacco distribuito, cioè originato contemporaneamente da diverse fonti (anche migliaia), per impedire il funzionamento di un servizio o di un'infrastruttura.

La potenza degli attacchi DDoS è data dalla quantità di *bot* coinvolti.

Un bot è costituito da un semplice pc o un server o un dispositivo connesso a internet che, una volta hackerato, è utilizzato dai cybercriminali per comporre una *botnet*. La rete così creata viene quindi utilizzata per sferrare un potente attacco cyber a un'infrastruttura o a un servizio.

Per le sue caratteristiche (i componenti della botnet non si rendono nemmeno conto di essere utilizzati a tale scopo), questo tipo di attacco è temutissimo e praticamente impossibile da contrastare. Il consiglio che gli esperti forniscono è di chiudere tutto e riaccendere la rete in un secondo tempo.

Quando un servizio destinato a moltissimi utenti non funziona (come può accadere per servizi come PayPal, WhatsApp, ecc.) è assai possibile che lo stesso sia sotto attacco DDoS.

Chi lo subisce non ha altra scelta che resettare, cioè calare le saracinesche e ricominciare da capo, il che comporta i problemi che ciascuno di noi può immaginare, trattandosi di sistemi che gestiscono comunicazioni e pagamenti tra milioni di persone, a livello davvero globale.

(continua a pag. 2)

(continua da pag. 1)

Per quanto ci si sforzi di tenere sotto controllo la sicurezza dei propri sistemi, non è possibile gestire l'operatività di un così alto numero di utenti e questa è l'arma che utilizza chi sferra tale tipo di attacchi.

UN RISCHIO NON QUOTABILE PER LE COMPAGNIE

Si tratta dell'ennesima ripercussione della guerra che sta interessando l'Europa (a questo punto è abbastanza limitativo dire che si tratti della sola Ucraina, per quanto, per nostra grande fortuna, i Paesi dell'Ue siano coinvolti a livello indiretto).

A quanto pare, a partire dai primi giorni dello scorso maggio, il Csirt ha registrato un'intensificazione degli attacchi di questo tipo contro soggetti nazionali e internazionali.

In seguito a ciò, è stato potenziato il monitoraggio di questo tipo di minaccia, attraverso l'identificazione delle attività di *probing* ai danni delle misure di protezione attive all'interno dei nostri sistemi.

Le attività di probing sono per lo più costituite da tentativi di sondaggio del funzionamento dei sistemi stessi da parte degli attaccanti. Tali attività, pur risultando al momento di bassa intensità, potrebbero preludere a successive azioni di attacco DDoS, con gravi conseguenze per i servizi e le infrastrutture oggetto dell'attacco stesso e per milioni di loro fruitori.

In poche parole, gli attacchi DDoS sono abbastanza difficili da sferrare, ma il risultato per i cybercriminali è assicurato.

Per tale ragione, questo evento è sempre escluso dalle polizze di assicurazione che coprono il cosiddetto *cyberisk*, perché le conseguenze che ne potrebbero derivare sono decisamente difficili da quantificare e sarebbe praticamente impossibile valutare questo tipo di rischio e predisporre una tariffa adeguata.

Il fatto che le attività di mitigazione e gestione dello stesso siano assai limitate, se non addirittura inesistenti in alcuni casi, determina infine l'impossibilità di fornire una qualche copertura da parte degli assicuratori.

COME È STRUTTURATA LA CYBER SICUREZZA ITALIANA

In questo clima di autentica cyberwar, il Comitato interministeriale per la cybersicurezza, presieduto dal presidente del Consiglio dei ministri, ha finalmente deliberato la *Strategia nazionale di cybersicurezza 2022-2026*, che comprende numerose iniziative, tra cui una serie di azioni per il potenziamento della resilienza nella transizione digitale del nostro Paese, il raggiungimento dell'autonomia strategica sul piano cibernetico, la gestione delle crisi cibernetiche e la lotta alla diffusione delle *fake news*.

Tale provvedimento rappresenta il completamento dell'attuazione normativa del *Perimetro di sicurezza nazionale cibernetica*, lo strumento ideato quale vero e proprio scudo difensivo italiano contro i cyber attacchi che minacciano le aziende e la pubblica amministrazione, entrato in vigore già a partire dalla fine del 2020, con il dpcm 131/2020.

Come abbiamo avuto modo di illustrare a suo tempo, il Perimetro di sicurezza nazionale cibernetica si rivolge principalmente a due categorie di soggetti:

a) quelli che esercitano una funzione essenziale dello Stato, ovvero coloro che sono destinati ad assicurare la continuità dell'azione di governo e degli organi istituzionali, la sicurezza interna ed esterna, la difesa, le relazioni internazionali, l'ordine pubblico, l'amministrazione della giustizia e la funzionalità del sistema economico, finanziario e dei trasporti;

b) quelli che prestano un servizio essenziale per gli interessi dello Stato, ovvero tutti i soggetti (siano essi pubblici o privati), che assicurano il mantenimento delle attività civili, sociali ed economiche fondamentali, esercitando attività necessarie per l'esercizio e la salvaguardia dei diritti fondamentali dei cittadini (come garantire la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica), o esperiscono attività di ricerca che presentino particolare rilievo ai fini dello sviluppo del sistema economico nazionale.

GARANTIRE LO SCAMBIO DI INFORMAZIONI

Si tratta, insomma, di garantire la resilienza di servizi informatici che non sono solo rilevanti per la sicurezza del nostro Paese, ma risultano indispensabili per l'esercizio di attività essenziali per i cittadini, sia per l'ammontare delle informazioni che vengono scambiate attraverso di essi, sia per la densità del loro utilizzo nella vita di tutti i giorni.

Si pensi all'uso che ognuno di noi fa di WhatsApp o al numero di transazioni economiche effettuate per il tramite di PayPal, per citare solo alcune delle infrastrutture oggetto dell'interesse degli hacker che potrebbero essere intenzionati a sferrare un attacco DDoS.

Per quanto il Perimetro sia stato ideato proprio per affrontare questo genere di crisi, è davvero difficile immaginare che i suoi artefici avessero previsto quanto si sta verificando in questo momento in Europa e nel mondo.

Cinzia Altomare

INSURANCE Daily

LUNEDÌ 13 GIUGNO 2022 N. 2181

INTERMEDIARI

Anagina, gli agenti diventano azionisti di Generali

Il presidente Davide Nicolao ha annunciato che la Cassa di previdenza ha acquistato 750mila azioni, con un investimento complessivo di 13 milioni di euro. L'obiettivo è avere un rappresentante in cda

Davide Nicolao, presidente di Anagina

Gli agenti di **Anagina** diventano azionisti di **Generali**. L'annuncio del presidente dell'associazione, **Davide Nicolao**, all'apertura dei lavori dell'89esima assemblea che riunisce 350 agenti, 3.500 dipendenti e 9.000 collaboratori, con una raccolta premi che nel 2021 ha raggiunto i 4,2 miliardi di euro, secondo quanto riporta una nota di Anagina.

Nicolao ha annunciato che la Cassa di previdenza di Anagina ha acquistato a oggi 750mila azioni Generali con un investimento complessivo di 13 milioni di euro e che gli acquisti proseguiranno nei prossimi giorni fino a raggiungere l'obiettivo di un milione di titoli.

"Al consiglio direttivo della Cassa di previdenza – continua la nota – sarà proposto di accantonare anche nel bilancio 2023 una somma da destinare all'acquisto di un altro pacchetto di titoli del Leone di Trieste".

Ma non basta, perché gli agenti Anagina hanno confermato il loro desiderio di avere un proprio rappresentante nel cda, come ai tempi degli agenti-imprenditori dell'ex Ina.

Sulla governance, ha parlato anche il group ceo **Philippe Donnet**, intervenuto al congresso con un messaggio video. "Dopo l'assemblea degli azionisti di fine aprile", ha detto, Generali può far leva "su una governance oggi all'altezza delle grandi public companies internazionali".

L'amministratore delegato della compagnia ha ringraziato gli agenti Anagina "per il supporto manifestato negli ultimi mesi e per il grande lavoro, la passione, l'energia" dimostrati nel lavoro quotidiano. Oggi Generali vanta 67 milioni di clienti in 49 Paesi.

All'assemblea degli agenti imprenditori del gruppo Anagina hanno partecipato, tra gli altri, anche la presidente dell'**Ania Maria Bianca Farina**; il presidente dell'**Abi**, **Antonio Patuelli**; il viceministro dello Sviluppo economico **Gilberto Pichetto Fratin**; e l'economista americano **Allen Sinai**.

Fabrizio Aurilia

CARRIERE

Double S saluta Maurizio Cappiello

Conclusa la collaborazione fra il manager e la società di brokeraggio

Maurizio Cappiello

Lo scorso 31 maggio si è conclusa la collaborazione fra **Maurizio Cappiello** e **Double S Insurance Broker**. Il presidente e amministratore delegato **Stefano Sardara** ha evidenziato in una nota "i risultati raggiunti ad oggi sotto il profilo organizzativo, quali la certificazione *ISO 9001*, la definizione del *Modello 231*, la struttura IT aziendale, la struttura del Tpa a servizio dei partner della società, gli accordi di comunicazione del brand Double S".

Tutti passaggi che la nota definisce "significativi per la struttura organizzativa della società, che hanno consentito alla Double S di fare un passo quantico dopo la trasformazione in società per azioni". Esaurite quindi le attività prefissate, prosegue la nota, "la Double S ringrazia sentitamente il dott. Maurizio Cappiello e il suo team per l'ottimo lavoro svolto, con professionalità, dedizione e nei tempi prefissati. A Maurizio – conclude il comunicato stampa – i migliori auguri per il prossimo futuro professionale e personale".

G.C.

INSURANCE Daily

LUNEDÌ 13 GIUGNO 2022 N. 2181

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