INSURANCE Daily

● GIOVEDÌ 23 APRILE 2020 N. 1737

PRIMO PIANO

Covid-19, una perdita storica

La pandemia di coronavirus potrà generare la più grande perdita nella storia dell'industria assicurativa. A dirlo, secondo quanto riportato dalla Reuters, è Evan Greenberg, ceo di Chubb, intervenuto ieri nel corso di una call con gli analisti per illustrare i risultati della compagnia nel primo trimestre dell'anno. La pandemia, come spiega una nota di Chubb, non ha al momento intaccato i conti della società: la compagnia non esclude tuttavia che quella che viene definita come "una catastrofe globale" possa avere "un impatto significativo sulle entrate, così come sul risultato netto e operativo nel secondo trimestre e, potenzialmente, nei successivi trimestri". A detta di Greenberg, "siamo di fronte a un momento senza precedenti di portata storica". Il ceo di Chubb si è quindi soffermato sulle pressioni arrivate dalla politica per spingere le compagnie a indennizzare le perdite che le imprese dovranno sostenere a seguito del lockdown imposto per prevenire la diffusione del virus, sebbene epidemie e pandemie siano spesso escluse dalle condizioni di polizza. "Tutto ciò potrebbe danneggiare o distruggere l'industria assicurativa in maniera terribile", ha affermato Greenberg. "Significherebbe – ha aggiunto – togliere semplicemente denaro a qualcuno per darlo a qualcun altro".

G.C.

RICERCHE

L'industria del ransomware

Anche l'operato di hacker e criminali informatici evolve verso modelli di business più maturi: le attività si strutturano in una sorta di supply chain, l'offerta di servizi (se così si possono definire) passa dai meandri del dark web. E così, secondo un rapporto di CyberCube, gli attacchi informatici assumono dimensioni ben più grandi di quelle a cui siamo abituati


© Tomasz Zajda | Fotolia

Nel pomeriggio dell'11 maggio 2017 il virus *WannaCry* infetta centinaia di migliaia di computer in tutto il mondo. Vengono colpiti i sistemi informatici del sistema sanitario britannico, così come le infrastrutture digitali di società come **FedEx**, **Renault** e **Telefónica**. Tutti i dati dei computer infettati vengono bloccati. Sul monitor compare una richiesta di riscatto: le informazioni e le funzionalità del terminale torneranno pienamente disponibili dietro il pagamento di un riscatto di 300 dollari in bitcoin, poi alzato a 600 dollari. Quel giorno la parola *ransomware* diventa di dominio pubblico.

Poco più di due anni e mezzo dopo, il 31 dicembre 2019, la società di cambio **Travelex** mette offline tutti i propri siti e le proprie app per dispositivi mobile a seguito di un attacco hacker. Una settimana dopo, ancora in pieno black-out, la società rende noto di essere rimasta vittima di un ransomware: il riscatto viene fissato a sei milioni di dollari. I sistemi vengono ripristinati soltanto intorno alla metà di gennaio. La società, che non sappiamo se abbia pagato o meno il riscatto, ha stimato per il primo trimestre dell'anno un calo delle entrate quantificabile in 32 milioni di dollari.

Come siamo passati in appena due anni da WannaCry a Travelex? Come è stato possibile passare da un attacco su vasta scala, che ha sostanzialmente sparato nel mucchio nella speranza di raccogliere poche centinaia di euro a computer, a un unico tentativo milionario indirizzato verso una singola società? Secondo **CyberCube**, che ha recentemente pubblicato il rapporto *Understanding ransomware trends*, tutto ciò è stato possibile perché hacker e criminali informatici hanno semplicemente modificato e fatto evolvere il proprio modello di business.

(continua a pag. 2)

INSURANCE Daily

GIOVEDÌ 23 APRILE 2020 N. 1737

(continua da pag. 1)

UN CRIME IN EVOLUZIONE

Alla base di tutto c'è in primo luogo una constatazione di semplice buon senso: imprese ed enti governativi hanno maggiori disponibilità rispetto a un semplice cittadino. "I criminali informatici hanno compreso che richieste di riscatto milionarie sono realizzabili quando l'obiettivo è una corporation, non un consumatore", si legge nel rapporto. Nel 2016, secondo **Symantec**, il cosiddetto *enterprise ransomware* copriva il 31% degli attacchi, mentre tutto il resto (69%) era costituito da offensive verso semplici cittadini. Nel 2018 i rapporti si erano praticamente ribaltati: gli attacchi alle imprese erano arrivati a quota 81%.

A ciò si aggiunge poi il fatto che imprese ed enti governativi hanno molto più da perdere rispetto a normali cittadini: oltre al semplice riscatto, danni ingenti possono derivare dalla perdita di proprietà intellettuali e di dati personali della clientela. L'evoluzione tecnologica, in questo contesto, si è mossa proprio nella direzione di trasformare queste debolezze in un'arma di ricatto in più per hacker e criminali informatici. "Sono state sviluppate una serie di campagne ransomware più avanzate, in cui i dati vengono sottratti prima ancora di essere crittografati sulla rete dell'istituzione posta sotto attacco", osserva il rapporto. Negli ultimi anni si sono già registrati casi in cui, a seguito del mancato pagamento del riscatto, l'attacco si è concluso con la pubblicazione dei dati che erano stati sottratti. Tutto ciò, unito anche alle disposizioni del *Notification Act* negli Stati Uniti e del *Gdpr* nell'Unione Europea in materia di *data breach*, ha probabilmente spinto hacker e criminali informatici a dirigere la propria attenzione verso imprese ed enti governativi.

RANSOMWARE AS A SERVICE

In passato il cyber crime era poco più di un'attività artigianale: tutto era in mano al singolo hacker, che preparava il virus, predisponeva l'attacco e, se le cose andavano nel verso giusto, raccoglieva i frutti del proprio lavoro. Adesso le cose sono cambiate. E il cyber crime, da semplice artigianato che era, si è trasformato in una vera e propria industria. Il modello di business risulta completamente differente. Il sistema è strutturato come una sorta di supply chain: ognuno ha il proprio ruolo all'interno della catena. E se l'attacco va a buon fine, i guadagni sono suddivisi fra tutti i partecipanti.

Nel settore ha fatto capolino anche una sorta di brokeraggio del crimine. Intermediari del cyber crime lavorano nei meandri del *dark web* e offrono ai propri clienti i loro servizi (se così si possono definire): virus e altri dispositivi che non richiedono particolari competenze tecnologiche per dar vita a un attacco informatico. Il rapporto, mutuando una locuzione tipica del linguaggio dell'informatica, parla a tal proposito di *ransomware as a service*.

INGEGNERIA SOCIALE E INTELLIGENZA ARTIFICIALE

L'evoluzione del settore, tuttavia, non si ferma certo qui. Il rapporto evidenzia, per esempio, una crescita inaspettata di pratiche di *social engineering*, forma di crimine informatico che sfrutta l'ingenuità e la scarsa attenzione degli utenti per spingerli a cedere informazioni personali come password o dati bancari. Negli ultimi tempi si è notata la tendenza a sfruttare eventi di attualità, come la pandemia di coronavirus, per spingere i bersagli a cliccare su link o scaricare allegati che attivano un attacco ransomware.

Lo sviluppo dell'intelligenza artificiale potrà dare nuova linfa al settore. Secondo il rapporto, hacker e criminali informatici nei prossimi anni potranno essere in grado di elaborare algoritmi estremamente efficaci nell'individuare il bersaglio e nell'indurlo a spingere il tasto giusto (per chi effettua l'attacco). "I criminali informatici sono bravi in social engineering, ma l'intelligenza artificiale lo sarà molto di più", si legge nel rapporto.

IL RUOLO DELLE ASSICURAZIONI

Il futuro dell'industria dei ransomware sembra già scritto: attacchi più mirati e strutturati, magari meno frequenti, ma dalle potenzialità devastanti. Se n'è già avuta qualche prova. Lo scorso anno, per esempio, un attacco ransomware ha bloccato per più di un mese le infrastrutture informatiche della città di Baltimora, negli Stati Uniti, provocando perdite per più di 18 milioni di dollari. Nel 2016, altro esempio, la **National Ink and Stitch** si decise a pagare il riscatto per riavere accesso ai propri sistemi informatici: gli autori dell'attacco non si accontentarono e fecero immediatamente una nuova richiesta di denaro.

Tutto ciò, come specifica il rapporto, "costituisce soltanto la punta dell'iceberg: molti attacchi vengono denunciati soltanto se coinvolgono dati sensibili o se possono comportare un danno di immagine". Ecco perché, secondo CyberCube, è necessario che le assicurazioni si impegnino a comprendere a fondo l'evoluzione della minaccia. "Sfruttare una vasta gamma di dati e competenze può aiutare gli assicuratori a ridurre l'incertezza data dall'esposizione a un rischio così grande e complesso", si legge nel rapporto. "Tutto ciò – prosegue nelle battute finali – può sostenere gli assicuratori non solo nel ridurre la loro incertezza, ma nel creare anche una base più sostenibile per rinnovare e creare soluzioni in materia di rischio informatico".

Giacomo Corvi

INSURANCE Daily

● GIOVEDÌ 23 APRILE 2020 N. 1737

DALLE AZIENDE

Team working e Covid-19: serve la leadership emotiva

Allo shock dei primi giorni di chiusura e lavoro a distanza è subentrato nelle settimane un sentimento di scoramento e incertezza per il futuro. Il confronto con colleghi e collaboratori deve tenere in considerazione lo stress che stiamo vivendo

L'emergenza sanitaria, che ha obbligato le persone a rivedere le proprie modalità di lavoro da un giorno a un altro, può essere vista anche come un'opportunità per osservare l'evoluzione delle dinamiche all'interno dei team in tempo di crisi. Sia per provare a migliorare i processi "in corsa", sia per apportare dei miglioramenti in prospettiva per quando l'emergenza sarà finita. Ma come sono cambiati i comportamenti delle persone nelle diverse fasi della crisi fino a oggi? E quali sono le soluzioni per mantenere un management efficace?

L'inizio della crisi Covid-19: concentrazione sul "Cosa"

La prima reazione è stata quella di considerare il *remote working* come una situazione temporanea. Perciò le persone si sono concentrate velocemente sulle attività che erano già in corso. In questa fase, paradossalmente si sono riscontrati degli effetti addirittura positivi: migliore efficienza nella gestione delle attività, maggiore sintesi e focalizzazione, migliore capacità di gestire le riunioni e più rapido allineamento sulle priorità immediate. Si è visto anche un maggior spirito solidale nell'aiutare i colleghi più in difficoltà con l'utilizzo di dispositivi e piattaforme digitali.

La variabile Tempo: concentrazione sul "Come"

Il protrarsi della crisi ha iniziato a lasciare spazio a emozioni diverse, spesso spiacevoli, legate a una maggiore incertezza.

(continua a pag. 4)

INSURANCE Daily

● GIOVEDÌ 23 APRILE 2020 N. 1737

(continua da pag. 3)

Le persone hanno manifestato due tipi di reazione, diametralmente opposti: c'è chi ha continuato a portare avanti le sue attività nella convinzione che in un tempo relativamente breve si tornerà alla normalità ("andrà tutto bene") e c'è chi è entrato in un vortice emotivo di paure legate al proprio futuro, sia dal punto di vista professionale (produzione ferma, azienda chiusa, ferie imposte o cassa integrazione), sia dal punto di vista personale (salute propria o dei propri cari).

Può accadere, in questo periodo, che le persone inizino a farsi sopraffare dalle emozioni. Continuano a chiedersi come e quando ne usciranno, e questo porta a cercare un numero sempre più elevato di dati e informazioni nel tentativo, spesso vano, di darsi delle risposte. Ma le informazioni, per essere davvero utili, devono essere trasparenti, chiare e provenire da fonti affidabili.

La soluzione sta nel riconoscere e accogliere le emozioni, anche quelle spiacevoli. Basta una semplice domanda: "Che cosa sto provando in questo momento?", a cui dare una risposta autentica. Dare un nome all'emozione è il primo passo per prendere atto di quale sia la situazione. Si inizia ad accettare, quindi, una *nuova normalità* ed è questo l'elemento base per arrivare al cambiamento, a livello razionale e soprattutto a livello emotivo. L'accettazione è il passaggio indispensabile per generare nuove alternative, nuove modalità per affrontare la realtà. Altro passaggio fondamentale, che permette al team di evolversi attraversando le difficoltà, è la fiducia. E qui entra in gioco il leader.

La soluzione per la resilienza del Team: concentrazione sul "Perchè"

In questo momento un leader capace ed efficace nel gestire l'operatività delle persone potrebbe non essere sufficiente, serve un cosiddetto *leader emotivo*. Dopo il "cosa" del primissimo momento della crisi e il "come" della seconda fase, bisogna concentrarsi sul "perché", sul senso.

Il leader emotivo deve essere capace di ascoltare il suo team e di dargli la motivazione per cui continuare a perseguire l'obiettivo, per poter pensare al "dopo-crisi".

Questa transizione da leader operativo a leader emotivo, passa prima di tutto per l'analisi del proprio stato d'animo e delle alternative possibili. In che modo?

- ad esempio, dando dei micro-obiettivi (o step intermedi) che saranno necessari per raggiungere la meta che era stata stabilita prima che scoppiasse l'emergenza;
- tenendo in considerazione le emozioni proprie e dei componenti del team, senza nascondere le proprie vulnerabilità;
- comunicando in maniera sincera, trasparente ed empatica, senza edulcorare la realtà, ma nemmeno utilizzando toni drammatici;
- abbandonando la logica del controllo e fidandosi delle persone.

Questo passaggio permette di evitare il crollo emotivo dei collaboratori e, di conseguenza, il blocco totale delle attività a causa di possibili episodi di *burnout*. Non dimentichiamo che la negatività è contagiosa e può fare danni incalcolabili. Chi si lamenta continuamente, per esempio, dovrebbe essere arginato nelle riunioni di gruppo, per portare poi la conversazione a un livello privato in cui il leader deve cercare di ascoltare le emozioni che si celano dietro quella lamentela per trovare insieme delle soluzioni, emotive o operative che siano.

Anche in un contesto complicato come quello attuale, il *work life balance* deve essere, per quanto possibile, tutelato e considerato ancora di più come una leva indispensabile per la continuità del business.

Mariella Bisaccia
e ***Mirko Soprani,***
docenti del Master
in Management & Leadership Skills di Cineas

Il master è in partenza dal 4 giugno. I moduli del master - Innovazione & change management, Intelligenza emotiva e comunicazione efficace, Tecniche di negoziazione, Problem solving & decision making e Strategie di team working - sono frequentabili anche individualmente.
Maggiori informazioni su Cineas.it

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