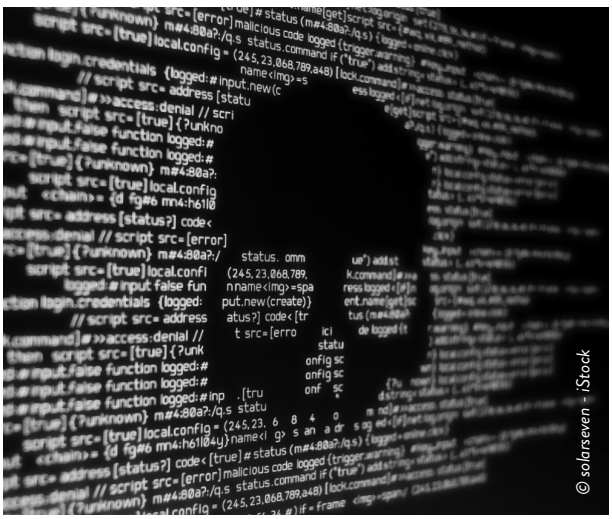
LA RISPOSTA A UN RISCHIO COMPLESSO

di CINZIA ALTOMARE

GLI ELEVATI COSTI PER SINISTRO, LA DIFFICOLTÀ DI DEFINIRE PARAMETRI EFFICIENTI E L'IMPREVEDIBILITÀ DI UNA MINACCIA CHE RIGUARDA TUTTO E TUTTI: OFFRIRE SOLUZIONI ASSICURATIVE PER IL CYBER RISK SI STA RIVELANDO PARTICOLARMENTE COMPLICATO. E IL MERCATO, POSTE QUESTE BASI, CONTINUA A SCONTARE UN ELEVATO GAP DI PROTEZIONE

Il mondo dei rischi che assicuratori e assicurati si trovano ad affrontare è costituito da un universo in espansione, una realtà in continua evoluzione, soggetta a cambiamenti che si verificano a un ritmo sempre più accelerato. Si tratta dei cosiddetti *rischi emergenti*, il cui potenziale di danno si può cercare di prevedere ma è difficile da calcolare: una vera e propria *materia oscura* per attuari e sottoscrittori, che cercano di destreggiarsi come possono, tentando di elaborare modelli di previsione per affrontarla. Come sappiamo, un rischio si può considerare assicurabile quando sia possibile parametrarlo, e molti rischi che oggi conosciamo, e siamo in grado di valutare e parametrare, sono stati rischi emergenti in un passato più o meno lontano. Da qualche tempo a questa parte, però, è lecito chiedersi se il rischio rappresentato dalla cosiddetta *minaccia tecnologica* o *cyber risk* sia un rischio tuttora catalogabile come *emergente* e, soprattutto, se si tratti di una fattispecie che sia davvero possibile assicurare. Come sappiamo, da alcuni anni esso costituisce la maggiore preoccupazione di tutti i risk manager, che lo hanno a più riprese collocato ai primissimi posti delle classifiche dei pericoli percepiti come gravi, o addirittura fatali, per le loro aziende. Se da un lato gli hacker utilizzano tecniche di estorsione sempre più evolute e gli attacchi informatici sono sempre più gravi e sofisticati, dall'altro la crescente digitalizzazione rende gli utenti e le infrastrutture sempre più vulnerabili, con ricadute che arrivano fino all'interruzione di



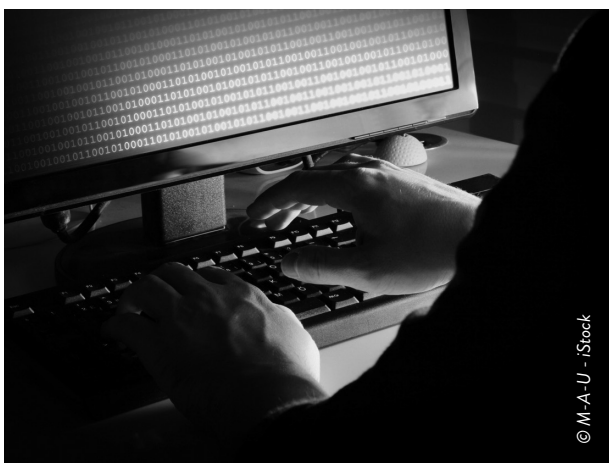
servizi essenziali, come la fornitura di acqua o energia. L'aumento degli attacchi informatici ha elevato la consapevolezza del rischio e quindi la domanda di protezione assicurativa, ma il cyber risk si caratterizza per la difficile quantificazione delle potenziali perdite e per lo scenario sempre in rapida evoluzione.

CYBER RISK INASSICURABILE?

Ogni singolo attacco cyber può avere impatti devastanti sul portafoglio di un assicuratore, con danni di tipo sistemico difficilmente sostenibili. Ciò rende questa fattispecie di rischio assai poco assicurabile e restrin-

ge la capacità del mercato, generando un altissimo gap di protezione. I premi assicurativi globali, infatti, dovrebbero aver raggiunto l'ammontare di 10 miliardi di dollari, e le previsioni degli osservatori parlano di una crescita annua del 20%, fino a raggiungere l'importo di circa 25 miliardi di dollari entro il 2025. Tuttavia, considerando che i danni globali ammonterebbero già a circa 945 miliardi di dollari, questi premi risulterebbero pari a una piccolissima frazione delle perdite annuali.

Da più parti, quindi, si è cominciato a sostenere che il cyber risk sia effettivamente *inassicurabile* e la potenzialità letale di questo tipo di danni sta spingendo gli assicuratori a porre significativi paletti, in termini di condizioni e limiti assicurativi. Conseguentemente, alcune voci che caratterizzano questo rischio, e che risultano essere le più temute dai risk manager, risultano escluse o fortemente limitate nei contratti assicurativi disponibili, il che impedisce una maggiore produzione di queste polizze, riportandoci al problema evidenziato: non sembrano esserci capitali sufficienti a sostenere l'assicurabilità del cyber risk. D'altro canto, il mercato necessita di una soluzione, sia per l'esorbitante ammontare dei danni sofferti, sia per l'esigenza di fronteggiare quanto la legislazione comunitaria impone a tutte le aziende sulla protezione dei dati sensibili: organizzare un piano di risk management per contrastare la minaccia tecnologica.



LA DEFINIZIONE DEL FENOMENO

Ma facciamo un passo indietro e partiamo dalla definizione del cyber risk. In pratica, parliamo di violazione di dati personali, intesi nel senso più ampio e comprendenti persone fisiche e giuridiche. Definiamo quindi questo tipo di rischio come un evento in cui dati sensibili e informazioni dei soggetti interessati (ad esempio, quelle mediche o finanziarie) vengono messi a rischio. Nell'ordinamento europeo questi dati sono concepiti come una parte integrante della persona stessa. Pertanto, quando gli stessi vengono persi o sottratti, riconosciamo tale perdita come un grave danno personale, alla stregua di un danno fisico. Pensiamo ad esempio agli archivi di tutte le società, nei quali i nomi dei clienti sono associati alle informazioni sulle loro carte di credito, oppure alle informazioni mediche conservate da assicuratori, medici e ospedali.

Dobbiamo ora tenere conto del fatto che la tecnologia ha ridefinito i confini della nostra società e vivere significa integrarla in ogni aspetto della nostra vita, all'interno di un *cyberspazio* in cui ci muoviamo e comunichiamo. I mattoni che formano tale spazio sono proprio le informazioni personali (parte integrante di quello che siamo, nella realtà in cui esistiamo), e questo ci rende suscettibili al rischio che esse vengano in qualche modo danneggiate o sottratte fraudolentemente. Tale vulnerabilità risiede nei nostri telefoni cellulari, computer, mezzi di trasporto, accessi agli istituti di credito e acquisti con carte di credito, in definitiva in tutti i dispositivi intelligenti presenti nelle nostre case e nei luoghi in cui lavoriamo.

HACKER E CRIMINE INFORMATICO

All'origine delle violazioni di dati ci sono generalmente le frodi informatiche (ovvero gli attacchi dolosi), ma è possibile che si verifichino anche problemi tecnici e perfino semplici errori umani. Quando le violazioni sono compiute artatamente, cioè per mano dei cosiddetti cybercriminali o hacker, le informazioni personali vengono sottratte e usate con scopi diversi (ma sempre illegalmente), e si stima che si verifichi un attacco hacker ogni 39 secondi.

Tecnicamente, oltre al generico *cybercrime* (furto di

dati per trarne vantaggi politici, economici o finanziari), gli attacchi più comuni possono prevedere:

- la *diffusione* (accesso ai sistemi per propagazione massiva, come accade per lo *spam*, e dunque l'intento è solitamente commerciale);
- l'*hacktivism* (diffamazione di organizzazioni o divulgazione di dati riservati, e dunque l'intento ha origine politica);
- il *furto di identità* (sottrazione di informazioni personali dei cittadini, con differenti intenti);
- la *distruzione o cancellazione materiale* dei dati, volta a ostacolare e danneggiare gli affari di una determinata azienda.

Non parliamo di questioni lontane anni luce dalla nostra vita quotidiana, come poteva sembrare ai primi osservatori di questo fenomeno, ma di casi che ci riguardano da vicino. Nel nostro paese, ad esempio, si sono verificati attacchi gravi alle strutture ospedaliere e universitarie e alle amministrazioni regionali. Alcuni mesi fa il Ced e i servizi informatici della Regione Lazio hanno subito un attacco *ransomware* (un attacco, cioè, che prevede la richiesta di un riscatto, per consentire alla vittima di ripristinare l'uso del sistema colpito) e ogni giorno si fa il punto sugli episodi, sempre più frequenti, di attacchi informatici alla sanità e alla pubblica amministrazione.

GUERRA E PANDEMIA

In seguito all'invasione dell'Ucraina e alla successiva *cyberwar* (un attacco informatico che ha come obiettivo un paese o le infrastrutture principali di una nazione), le nostre infrastrutture sono state prese di mira dagli hacker di entrambi gli schieramenti, al punto che il *Csirt* (Computer security incident response team), creato nel 2018 presso l'**Agenzia per la cybersicurezza nazionale**, ha emanato un bollettino sulle attività di preparazione di attacchi verso le nostre infrastrutture. È stata quindi registrata un'intensificazione di tentativi di violazione contro soggetti nazionali, ed è stato potenziato il monitoraggio di queste minacce, attraverso l'identificazione delle attività di *probing* ai danni delle misure di protezione attive all'interno dei nostri sistemi. Le attività di *probing* sono tentativi di sondaggio del funzionamento dei sistemi stessi da parte degli attaccanti e preludono a successive azioni di violazione, con gravi conseguenze per i servizi e le infrastrutture e per milioni di loro fruitori. Si tratta di attacchi con un impatto sistemico su ogni aspetto della società, della politica, dell'economia e della geopolitica.

Anche il fattore pandemia ha avuto una certa influenza. Secondo il rapporto del **Clusit**, il 10% degli attacchi portati a termine è stato concentrato sul tema del Covid-19 e diverse operazioni di spionaggio sono state compiute a danno di organizzazioni di ricerca correlate con lo sviluppo dei vaccini. Nel maggio del 2020, per esempio, è stato registrato un attacco noto come *NUOVA APP IMMUNI ANTEPRIMA*: il messaggio che gli utenti ricevevano invitava a installare nel proprio computer l'app *Immuni* per far fronte all'emergenza epidemiologica da un link presente all'interno del messaggio. Il link, in realtà, scaricava il ransomware deno-


© ismagilov - iStock

minato *Fuckunicorn* e, mentre lo stesso cifrava i file del malcapitato, veniva mostrata all'utente la schermata di una mappa raffigurante l'infezione da Covid-19 che dilagava. Il riscatto richiesto ammontava a 300 euro per vittima, da versare in *bitcoin*.

IL COSTO DI UN SINISTRO INFORMATICO

I costi degli incidenti informatici vengono generalmente divisi in due fasi, tra costi immediati e costi dilazionati, ovvero sostenuti in un secondo momento. La loro portata può variare notevolmente per settore e può essere influenzata da una serie di fattori, come il tipo di azienda mirata, i dati che la società gestisce e le implicazioni normative e legali dell'incidente. Ciò significa che attacchi informatici simili possono avere costi molto diversi, ma è certo che queste violazioni impattano sulla capacità di un'azienda di condurre la propria attività, comportando seri danni reputazionali e spese anche ingenti per recuperare i dati perduti e resistere alle eventuali azioni di risarcimento intraprese contro di essa (per non parlare di multe e ammende, che sono salatissime).

Al di là dei costi diretti, gli attacchi degli hackers possono anche causare accumulazioni di rischio estese alle società interdipendenti, attraverso la catena distributiva globale. Un attacco di media gravità può facilmente danneggiare l'intera catena produttiva di un'impresa, per l'uso estensivo di internet nell'intero sistema. Sono costi in grado di porre a rischio la solvibilità stessa di un'azienda. Secondo quanto riportato dall'**Ibm**, Il costo medio di una violazione di dati ammonta a circa 3,86 milioni di dollari e la cifra sale a 8,64 milioni di dollari se si analizzano solo i dati relativi agli Stati Uniti. La ragione della differenza risale alla maggiore complessità dei sistemi di sicurezza adottati negli Usa, perché è ormai provato che le spese di ripristino di sistemi meno accessibili sono assai più elevate. Il costo medio per ogni singolo record perso o rubato ammonterebbe a circa 150 dollari: se moltiplichiamo questa cifra per l'enorme numero dei dati che possono essere sottratti, è facile arrivare a importi ragguardevoli. Il *Breach level index* denuncia un costo medio di oltre 2,5 milioni di dollari per ciascun attacco virale e una spesa di quasi sei milioni di dollari per ogni perdita di informazioni subita da un'azienda attaccata. Se confrontiamo questi

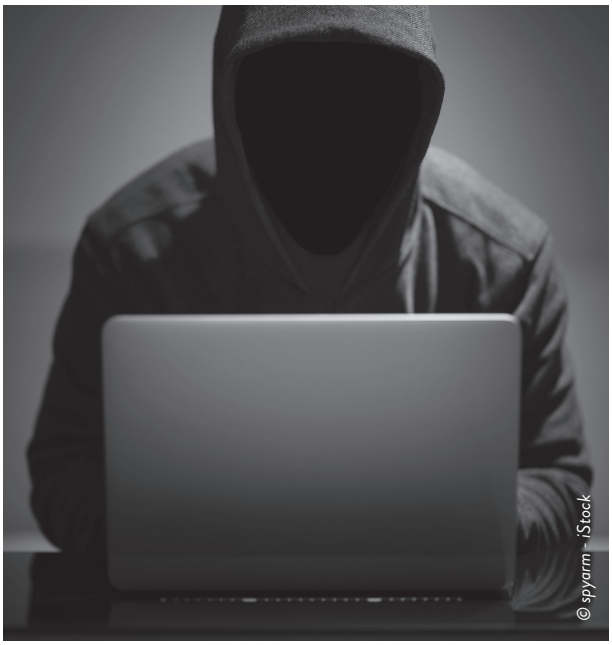
dati ai massimali e ai limiti di indennizzo offerti dagli assicuratori per le polizze che coprono il cyber risk, ci rendiamo conto di quanto gli stessi risultino inadeguati alla bisogna.

UN RISCHIO DIFFICILE DA PARAMETRARE

Ma come è possibile coprire un rischio praticamente impossibile da parametrare, i cui confini territoriali sono liquidi, come le frontiere che delimitano il cyberspazio nel quale si muovono le informazioni personali che ne costituiscono l'oggetto? Uno dei *data breach* più eclatanti dei quali abbiamo contezza è stato quello subito da **Yahoo** nel 2016. In questo caso oltre mezzo miliardo di account sarebbero stati violati. Gli attaccanti sottrassero nomi, indirizzi e-mail, numeri di telefono, date di nascita, password criptate e molto altro ancora. Il tutto sarebbe poi stato messo in vendita nel *dark web*, per circa 300mila dollari, ma secondo molti analisti finanziari, a causa di questo attacco, il valore della quotazione di Yahoo, che era in procinto di essere acquisita da parte di **Verizon**, si ridusse di circa 350 milioni di dollari.

Un attacco a **British Airways** nel 2018 costò alla compagnia aerea il 3% del suo valore azionario ed è facile individuare qui uno dei maggiori problemi che incontriamo quando cerchiamo di quantificare i danni derivanti da questo tipo di rischio: le aziende attaccate incontrano gravissimi problemi reputazionali e, una volta resesi conto di aver subito l'attacco (il che è tutt'altro che semplice, dato che può trascorrere molto tempo), hanno forti remore a denunciare il danno. Immaginatevi un istituto di credito che subisca un attacco massivo. Un report pubblicato qualche anno fa da **Marsh** rivelò che ben il 60% degli intervistati avrebbe dichiarato di voler trasferire immediatamente il proprio conto bancario se avesse saputo che il proprio istituto era stato hackerato.

Eppure, il regolamento europeo che definisce i principi


© spyarm - iStock

per il trattamento dei dati personali, il famoso *Gdpr*, stabilisce pene severe per chi non denunciasse immediatamente di aver subito un attacco, e le multe e ammende comminate dal garante per chi non avesse adempiuto ai numerosi requisiti, previsti per qualunque azienda che tratti dati sensibili, sono alquanto cospicue. Queste multe costituiscono una delle maggiori preoccupazioni di chi si occupa di sicurezza dei dati. Ma multe e ammende non sono assicurabili nella maggior parte delle giurisdizioni, e anche questo contribuisce a sottrarre *appeal* alle polizze offerte nei vari mercati, sempre ammesso che ancora si riesca a trovare compagnie in grado di sostenere i costi ai quali abbiamo fatto cenno, a un prezzo abbordabile per gli assicurati. E dunque la domanda resta aperta: a distanza di qualche decennio dalla sua emersione sui nostri radar, possiamo davvero considerare il cyber risk come un rischio parametrabile e quindi assicurabile?