IL RISCHIO CYBER C'È, VE LO ASSICURO...

L'epidemia di Cryptolocker e dei tanti altri ramsonware che ha indiscriminatamente colpito entità pubbliche e private di qualunque dimensione, cifrandone in modo fraudolento documenti e archivi, ha aiutato a far capire che un incidente informatico può toccare a chiunque

di UMBERTO RAPETTO
Generale (r) Guardia di Finanza - cyber security advisor

Non ho letto l'oroscopo ma qualche amico mi ha detto che per il segno del Leone l'anno sarà splendido.
In quel momento ho capito che i rischi cibernetici non sono nati tra il 23 luglio e il 22 agosto.
Ho persino pensato che il mio 2016 sarà ricco di soddisfazioni professionali perché anche Cnbc nel suo The world's biggest risks *mette i pericoli tecnologici in pole position tra le maggiori preoccupazioni dei mesi a venire.*
Molti non credono nelle influenze astrali e, a esser sincero, nemmeno io mi affido all'interpretazione di stelle e pianeti. Stavolta, però, il pronostico potrebbe essere azzeccato.
Tanti incrociano le dita, toccano ferro (o legno, secondo le diverse tradizioni), strofinano amuleti, si affidano a oggetti portafortuna. Qualcuno, forse meno scaramantico ma più previdente, ritiene che le strade da seguire possano essere altre.
L'itinerario, apparentemente tortuoso, in realtà prevede percorsi alternativi e suggerisce di non perdere alcun chilometro dei diversi tragitti. Le inevitabili tappe dell'ipotetico raid per mettersi al sicuro sono sostanzialmente sei: la formazione e la sensibilizzazione delle risorse umane ai diversi livelli, la redazione di norme comportamentali agili ma non elastiche, la previsione e l'implementazione di misure di sicurezza, la verifica dell'efficacia delle cautele adottate, la pianificazione delle modalità di contrasto alle emergenze e di ripristino della normalità, la copertura assicurativa.

La caccia al tallone d'Achille

Ancor prima di mettersi in cammino è forse opportuno procedere a una sorta di ricognizione tassonomica. Sembrerà strano, ma troppo spesso ci si dimentica di omogeneizzare il linguaggio e focalizzare lo scenario di intervento, rinunciando a un approccio ortopedicamente corretto alla questione e spesso precludendo la completa visibilità e idonea interpretazione del problema.
Il mondo assicurativo ha avuto il tempo di riconoscere

e metabolizzare i rischi "tradizionali", mentre ancora stenta a classificare con fluidità le insidie di carattere tecnologico. Gli occhiali con cui scrutare l'orizzonte devono permettere di distinguere in modo nitido le tipologie di possibili attacchi, i punti deboli, le presumibili conseguenze.

Gli attacchi sono inquadrabili in ragione della natura di chi se ne rende protagonista (attori State-sponsored, terroristi, aziende private concorrenti, organizzazioni criminali, attivisti, impiegati ed ex dipendenti, agenti isolati), del livello di sofisticazione o tecnicismo, della persistenza (breve e occasionale, automatizzata con una scansione non orientata a un bersaglio predefinito, duratura e mirata), della prossimità della fonte di aggressione (operatore interno con accesso diretto alla rete, accesso fisico ad apparati Ict di interesse, attacco a reti wireless debordanti il perimetro aziendale, azione offensiva dall'esterno con accesso da remoto o tramite internet), dell'eventuale origine non dolosa dell'incidente (inconvenienti o malfunzionamenti hardware o software, errori umani, fenomeni naturali…).

La caccia al tallone d'Achille porta dinanzi a una ovvia dicotomia. L'evento nocivo la cui manifestazione può innescare dinamiche risarcitorie può aver luogo all'interno dell'organizzazione dell'assicurato (lavoratore, dispositivo, sistema informatico, archivio, rete) oppure manifestarsi al di fuori di tale contesto (infrastrutture tecnologiche messe a disposizione dai provider, catena logistica di fornitori o partner non Ict, aree limitrofe alle sedi dell'impresa).

Le differenti varietà di danni che l'assicurato auspica siano indennizzati dalla compagnia assicuratrice: la gamma spazia dal furto di file protetti dalla proprietà intellettuale alle informazioni commerciali e industriali sensibili, dalla distruzione/interruzione dell'attività produttiva alla cancellazione o al danneggiamento di dati e programmi, dalle perdite finanziarie dirette alla sottrazione di fondi, dalle passività dei terzi (in cui rientrano clienti, dipendenti, azionisti…) alle azioni regolatorie, dalla rivelazione di dati appartenenti ai propri interlocutori professionali/commerciali/industriali al danneggiamento della reputazione e della credibilità sul mercato, dai non escludibili danni materiali o fisici a persone e cose agli inevitabili costi investigativi e di ripristino delle condizioni di normalità. L'elenco delle riverberazioni negative potrebbe proseguire in maniera impietosa.

Le alternative per il settore assicurativo

Business blackout *e* cyber-extortions *sono le parole chiave dell'anno appena cominciato. Quasi si parlasse di atelier e di sfilate, la moda 2016 del rischio si incardina su queste due pietre d'angolo.*

La paralisi infotelematica di una qualsivoglia realtà di impresa o la semplice cifratura indesiderata dei dati, ad opera di qualche pirata, sono eventi non solo possibili ma con una probabilità di accadimento quotidiana o addirittura oraria.

Alla base di tanta precarietà ci sono una sostanziale mancanza di sensibilità dei decision maker, l'incapacità di committenza del management che dovrebbe scegliere le soluzioni tecniche e organizzative per difendere l'azienda, l'impreparazione della forza lavoro. Uno scenario sconfortante, incorniciato dalla più solenne approssimazione tipica delle civiltà in declino.

Il pianeta insurance ha più alternative: riconoscere un ridotto interesse alla copertura di un simile rischio latore di potenziali bagni di sangue, imporre audit ferocissimi e condizioni hi-level di sicurezza che nessuno riuscirebbe a raggiungere, investire nella crescita culturale dei potenziali clienti mettendo a disposizione competenze in grado di generare in loro la necessaria affidabilità.

L'ultima opzione è forse quella da preferire perché il vero busillis non è individuare il prodotto assicurativo più smart, ma fare in modo che il proprio target commerciale sia ragionevolmente assicurabile e se ne possa avere una prova concreta fondata sulla condivisione delle conoscenze e degli obiettivi.

La buonanima di Max Catalano potrebbe sorridere dall'aldilà, ma il ragionamento è, purtroppo, non così scontato.