

UN'OCCASIONE DA NON PERDERE, O IN CUI SI PUÒ PERDERE?



di UMBERTO RAPETTO
 Ceo di HKAO Human knowledge as opportunity
 Generale (r) GdF, già Comandante del Gat Nucleo speciale frodi telematiche,
 docente universitario, giornalista e scrittore

Conosco automobilisti che non si preoccupano. "Tanto c'è l'assicurazione..."

Nel corso degli anni ho visto le compagnie attrezzarsi in modo sistematico per evitare situazioni in cui la nonchalance e, a volte, la furbizia dei propri clienti sono in grado di sorprendere anche i più avveduti redattori di modelli di rischio e matrici predittive.

Se truffe e frodi, nonostante il qualificato impegno riversato e le esperienze maturate, trovano sempre modo di insinuarsi anche in un contesto vaccinato, mi domando (e non credo di essere l'unico dinanzi a simile dilemma) come il mondo assicurativo potrà e dovrà affrontare la grande opportunità rappresentata dalle polizze a copertura dei rischi cibernetici.

La prospettiva di un nuovo mercato è senza dubbio allettante ma lascia intravedere significative difficoltà di calcolo. Il tentativo di determinazione puntuale di parametri di misurazione delle minacce digitali inciampa in una ampia varietà di possibili incidenti talmente vasta da scombinare qualsivoglia dinamica di computo.

Il primo serio ostacolo è quello della classificazione e della categorizzazione del rischio cyber, che può risiedere in qualunque momento e angolo dell'utilizzo di apparati e programmi informatici e di comunicazione.

Non basta considerare teoricamente la compromissione di riservatezza, disponibilità e integrità dei dati e dei servizi a questi correlati. All'orizzonte si profilano conseguenze di più immediata percezione, come la paralisi delle infrastrutture tecnologiche, la sostanziale distruzione del business, i danni materiali a persone e cose. Chi rifiuta ipotetici scenari apocalittici, non riesce però a schivare le tante e forse troppe drammatiche circostanze di quotidiana manifestazione che sono il risultato dell'adozione di cautele inadeguate a tutelare il regolare funzionamento di sistemi e reti di enti e aziende.

Dalle informazioni ai fattori di vulnerabilità

Non volendo considerare scenari di guerra o terrorismo e guardando solo a vicende ordinarie, normali, ci accorgiamo che qualsiasi organizzazione può finire sotto attacco da parte di soggetti determinati a rubare informazioni commerciali o a sottrarre segreti industriali, a recare danno o a rovinare la reputazione e la credibilità, a dar luogo a una frode o a estorcere denaro, a bloccare i sistemi informatici per vandalismo o per avvantaggiare un concorrente che ha commissionato l'operazione.

La platea dei malintenzionati è affollatissima. E agli hooligan che arrivano da fuori (terroristi, criminali più o meno organizzati, sabotatori, attivisti, concorrenti, ex dipendenti, troll e lupi solitari) vanno aggiunti i tanti e forse troppi individui pericolosi che a diverso titolo frequentano l'azienda: anche qui l'elenco è lungo perché si va dai dipendenti insoddisfatti o semplicemente incapaci, agli interinali sottopagati, ai consulenti pronti al doppio gioco e così a seguire.

Le informazioni solitamente richieste a chi sottoscrive una polizza si riducono a una manciata di minuzie insufficienti a fornire un quadro idoneo per le valutazioni necessarie.

Non basta sapere se l'assicurando ha dedicato specifiche risorse alla protezione dei dati (ad esempio un Cio, un cto o un cso, dove la C sta sempre per chief e la O per officer, e che nella fattispecie diventano uno information, l'altro technical e l'ultimo security), se sono state redatte regole, linee guida e procedure riferite alla sicurezza informatica, se esistono misure di difesa e precauzioni specifiche sul fronte It, se è stato previsto un piano di risposta a potenziali incidenti e di ripristino delle condizioni antecedenti, se il vertice aziendale è coinvolto e consapevole, se il personale è stato adeguatamente preparato a servirsi dei vantaggi degli strumenti tecnologici.

L'individuazione dei fattori di vulnerabilità e di conseguente rischio è un'operazione di non trascurabile complessità e dovrebbe essere preceduta dalla definizione esaustiva e classificazione puntuale delle possibili insidie e della relativa probabilità di accadimento.

Quando il software non basta

Il recente impulso, dato oltreoceano dal Dipartimento americano per la Homeland security all'universo assicurativo, ha innescato una repentina presa di coscienza che ha messo le grandi compagnie in bilico tra una chance irripetibile e una sorta di incubo. La promozione di un massiccio mercato di polizze e prodotti cyber (essenziale per rafforzare pubblico e privato alle

prese con le odierne minacce) purtroppo non si basa su una fertile base di conoscenze condivise su quel che è successo, sta accadendo o potrebbe verificarsi. L'information sharing è la condicio sine qua non, ma va a cozzare contro i pericolosi iceberg della privacy e della tutela dei non pochi segreti di Puccio d'Aniello (o Pulcinella) che caratterizzano la competitività aziendale.

L'anonimato dei dati riferiti a inconvenienti cibernetici deve essere ovviamente rispettato, ma la reticenza su come e quando non può trovare alcuna giustificazione e pregiudica una crescita adeguata in un ambito in cui il problema ha priorità assoluta.

I frequenti episodi di data breach, caratterizzati dall'accesso indebito a mastodontici archivi elettronici e dalla agevole esfiltrazione dei loro contenuti, massiva o selezionata, di informazioni personali, impongono di riflettere sui danni a soggetti terzi e sulla non remota ipotesi di class action mirate a risarcimenti di entità proporzionale al numero delle vittime e alla natura dei dati che ciascuno si è visto scappare o pubblicare. La diffusione di ransomware, capaci di dribblare molti antivirus e di criptare i documenti di un'azienda al solo improvvido clic di un impiegato su un venefico allegato alla mail, non ha risparmiato nemmeno le realtà che, tronfie ed altezzose, avrebbero compilato qualunque questionario prestampato. Si potrebbe continuare, ma fermiamoci qui.

Il busillis sta nel riconoscere l'assicurabilità di un possibile cliente, percorso che comincia con un'inquadatura grandangolare e con una analisi storica del settore in cui questo opera. Qualcuno confida in portentosi software Dss o in sistemi esperti capaci di pensare, stimare, suggerire. Sicuramente certe soluzioni possono sforbicare, ma il lavoro impone la finezza del rasoio nelle abili mani di un elegante barbiere di un tempo. La caccia a Figaro è cominciata e molti sedicenti coiffeur offrono già i loro servizi spacciando destrezza che non appartiene loro. Prima di farsi insaponare il volto, è consigliabile verificarne le referenze.