L’esposizione al rischio dei soft-target, un problema globale per soluzioni globali

a colloquio con Genseric Cantournet, Chaiman di Kelony International
a cura di Raffaello Juvara

L’episodio avvenuto nella prima serata del Festival di Sanremo 2018, con una persona salita sul palco durante la trasmissione, ha messo in evidenza due aspetti: l’esposizione dei grandi eventi ad ogni possibile azione dimostrativa, antagonista o, peggio, terroristica; l’esistenza di possibile falle nella sicurezza pubblica e privata preposta all’evento. Qual è la sua valutazione in merito?

Alcune osservazioni più che una valutazione. La sicurezza è una disciplina che è necessario approcciare sempre con obiettivi di tutela molto alti, proprio perché in gioco c’è la vita delle persone e la reputazione di Istituzioni nobilissime, di Infrastrutture Critiche e del nostro Paese. Il caso di Sanremo illustra che un’approssimazione nella valutazione del rischio o nell’applicazione delle misure di contrasto, non importa quale sia la causa, può essere potenzialmente fatale sia alle persone da tutelare sia all’Organizzazione che le mette in campo.

Di fronte a rischi sempre più pervasivi, i cosiddetti “soft-target” come il Festival di Sanremo sperimentano il fatto di dover prendere decisioni sempre più rapide in un contesto di incertezza sovrana con conseguenze radicali, e si trovano ad affrontare un ambiente sempre più volatile, incerto, complesso e ambiguo.

Di fronte a rischi sempre più iper-connessi e complessi dell’ecosistema normativo, giuridico, sociale, ambientale ed economico, non si può più trarre ispirazione dal passato ma si deve ripensare radicalmente il modello di

tema centrale in quello che è successo con l’intrusione sul palco del festival della canzone, spesso e volentieri non viene considerato nella sua interezza. Purtroppo, la sicurezza continua ad essere gestita in modo frammentato, secondo le varie discipline che la compongono. Da un punto di vista strategico, ma anche operativo, significa aggredire un avversario con forze sparse fin dall’inizio e creare inevitabilmente delle falle, dei gap.

A mio avviso, la sicurezza oggi non può che essere figlia della cindinica[1], con un approccio convergente, sistemico e preventivo. La scienza della prospettiva che non accada nulla, ossia che siano state preventivamente messe in campo le dovute competenze, tecniche e strumenti, con grande serietà. Questo è quanto era messo in opera quando ero Direttore della Security e della Safety in RAI. Portare attenzione alle falle di sicurezza, reali o percepite, è strategico perché sono portatrici di vulnerabilità. Si metta

1 Cindinica: scienza dello studio dei rischi

nei panni del possibile criminale che volesse colpire un bersaglio, o in ottica terroristica o anche semplicemente per creare scompiglio e insicurezza, quale sceglierebbe: quello apparentemente solido, oppure quello che dà segnali di livelli di tenuta approssimativi?

Come possiamo riuscire a tutelarci in questo mondo instabile e imprevedibile? L'obiettivo deve essere quello di anticipare i rischi e non di adattarsi ad essi o rincorrerli cercando di tamponare di volta in volta. È quindi necessario disporre di un protocollo di sicurezza convergente, basato sulla cindinica, che ha proprio questo scopo: rafforzare il livello di tenuta generale in modo sostenibile.

Alcuni fondamentali step, di un piano d'azione, per ottenere il dovuto successo sui rischi comprendono, per prima cosa, la definizione di una visione chiara come antidoto alla volatilità e all'incertezza. Solo la condivisione di proiezioni, unite a valori e strategie aziendali tra i vertici e il management, permette di orientarsi in un contesto carente di punti di riferimento o che sono stati annientati da situazioni rapidamente mutevoli.

Seconda cosa, affrontare i rischi necessita di una grande capacità di ascolto, soprattutto nei confronti dei cosiddetti «segnali deboli». Ascoltare per prevenirli, contrastarli e addirittura anticiparli e quindi capire quali esigenze richiederanno in futuro.

Terzo, adottare uno schema mentale flessibile per gestire la complessità. Ovvero, cosa non semplice in realtà, trovare soluzioni creative rispetto a nuove situazioni ed esigenze, ma anche riuscire ad interpretare correttamente le proprie incompletezze: non si tratta di cercare i «colpevoli», ma di trovare collettivamente i mezzi per evitare il ripetersi del problema incontrato. Questa pratica sviluppa collaborazione e performance.

Quarto ed ultimo, rimuovere le ambiguità dei paradossi odierni anche accettando di interrogarsi e non dare nulla per scontato, oltre che sviluppare grandi capacità di adattamento.

Il tutto richiede una spiccata propensione al cambiamento verso la sicurezza convergente e sistemica, e la capacità di prendere decisioni rapide. La sicurezza non è un gioco, e perdere non è contemplabile.

Si parla di sicurezza partecipata tra pubblico e privato che dovrebbe esprimere i massimi risultati proprio in situazioni simili, come, ad esempio, è avvenuto positivamente nel 2017 in occasione del concerto di Vasco Rossi a Modena. È possibile, secondo lei, parlare di linee guida ufficiali che facciano riferimento anche a best practices internazionali?

In termini di sicurezza viviamo in un grande paradosso. Da un lato sappiamo in modo pertinente che la sopravvivenza sta nell'adattarsi, nel cambiare più velocemente del cambiamento stesso; d'altro canto, siamo creature abitudinarie che si rassicurano ripetendo permanentemente le stesse procedure. Avere delle «best practices» da applicare indistintamente farebbe un gran comodo. Peccato che questo contraddica fortemente con il carattere dinamico dei rischi, inarrestabilmente incostanti e profondamente mutevoli.

Le due realtà non sono quindi compatibili. Più si vuole agire a largo spettro, più si diluisce la qualità dell'antidoto. Occorre quindi superare la logica dell'adempimento pedissequo alle «best practices» proprio perché negano il principio di adattabilità. La necessità è quella di migrare da una logica di obbligo di mezzi a quella di un obbligo di risultati. Ciò significa andare oltre la semplice focalizzazione dell'aspetto meramente formale e calare

intelligentemente le «buone pratiche» in ogni particolare realtà con un approccio necessariamente olistico.
Le numerose stratificazioni di norme, certificazioni e standard declinate in best practices sono dei prerequisiti, assolutamente utili ma non certo sufficienti: indicano la via ma non la meta, cioè come traguardare con un fattivo risultato di protezione effettiva.
Più che di best practices, i soft-target e le aziende in generale hanno bisogno del supporto di team internazionali ed interdisciplinari di comprovata esperienza. Internazionali perché si ottiene immediatamente una visione più ampia e più ricca dei rischi e, quindi, maggiori possibilità di prevenirli e contrastarli. Interdisciplinari perché l'unico approccio adeguato non può che essere olistico e convergente fin dall'inizio, per avere una chiara visione del rischio in tutte le sue sfaccettature. Non vederle significa non cogliere gli interstizi dove si nicchiano le vulnerabilità. La valutazione del rischio intercorrelato è uno degli strumenti cardini per ottenere questo risultato.

Come valuta l'estensione in atto dei compiti del security manager, figura professionale nata per proteggere i beni fisici delle imprese, che ora deve affrontare minacce totalmente diverse, dal terrorismo agli attacchi cyber ed ai rischi reputazionali sui social? Ritiene adeguati i profili dei professionisti della sicurezza definiti dall'attuale norma 10459 o dovrebbero esserci altre competenze? Com'è la situazione in Francia, ad esempio?
La Francia ha sempre sostenuto una visione giacobina della difesa. Così facendo, ha sempre promosso da un lato una grande attenzione al tema, dall'altro una visione accentratrice della sicurezza. Basti pensare all'Agenzia nazionale per la sicurezza dei sistemi d'informazione (ANSSI) o, più recentemente, alle Leggi di orientamento e programmazione per le prestazioni di sicurezza interna (LOPPSI I e II) oppure allo stato di emergenza, ancora applicato l'anno scorso in occasione degli attentati. Queste due ultime conferiscono alle istituzioni ed autorità poteri «esorbitanti» dal diritto comune che limitano le libertà individuali. Ossia la sicurezza collettiva prima delle libertà individuali, in un paese il cui motto inizia con «Liberté».
Questo non ha certo favorito le sinergie tra pubblico e privato. L'Italia è stata invece in questo avveniristica e lungimirante, e la norma UNI 10459 è una delle fattive dimostrazioni. Partecipai all'aggiornamento della norma in UNI e ritengo che i profili dei professionisti della sicurezza siano più che adeguati, a patto che l'aggiornamento previsto dalla norma stessa sia effettivamente svolto. È, quindi, necessario aggiornare regolarmente sia la norma che i profili dei professionisti coinvolti con le competenze richieste. Ricordando però, sempre, che le norme sono un punto di partenza e non di arrivo. Avere la patente di guida non esenta da possibili incidenti stradali. È solo un prerequisito necessario ma non sufficiente. Solo seguendo questa logica i responsabili della sicurezza, in tutte le sue accezioni, saranno in grado di affrontare l'estensione dei loro compiti che rispecchia quella dei rischi, sia in ampiezza delle tematiche impattate, sia in pervasività.
Più che di altre competenze, quindi, c'è urgente bisogno di modificare l'approccio alla sicurezza. Non basta più «essere compliant» oppure pensare di «essere ben coperti» dai rischi. Bisogna verificarlo nei fatti con il parametro della terzietà indipendente. Tutte le cose importanti della vita normalmente si affrontano secondo questa logica, cioè un terzo di fiducia che verifica non solo la realtà delle cose ma anche della loro bontà. Se ci pensiamo, ciò avviene per i flussi finanziari che transitano tramite una banca o una Blockchain, per i bilanci aziendali che vengono verificati da revisori preposti, per l'acquisto di un asset immobiliare che necessita la presenza di un Notaio, ecc. E per la «sicurezza»? Serve quindi un approccio convergente e globale, coadiuvato da un metodo di calcolo del rischio intercorrelato – come il protocollo SeVeVa™[2] - e da un ente terzo di fiducia per la verifica e la validazione dei processi di tutela.

2 Protocollo algoritmico proprietario basato su una metodologia convergente e interdisciplinare, che permette di rilevare e classificare tutte le tipologie di criticità, tramite l'analisi e la misura del grado di interdipendenza tra i rischi. In particolare, consente di intercettare le interconnessioni tra di essi e individuare preventivamente il pericoloso effetto domino.