Sicurezza e Sistema Paese: non solo cybercrime

Sempre più spesso si dibatte di sicurezza informatica e cybercrime, finendo con il non considerare gli attacchi fisici. È la cosiddetta strategia della lumaca, in riferimento al caso accaduto in Giappone nel maggio scorso, quando una lumaca, dopo essersi infilata in una centralina elettrica di una stazione, ha causato un cortocircuito e la sospensione del traffico ferroviario. L'analisi a cura di Securesat.

Mentre i media e gli addetti delle grandi aziende si concentrano su sicurezza informatica, cybercrime, minacce e attacchi hacker e ci si interroga sulla vulnerabilità dei sistemi di controllo industriali definendoli estremamente attaccabili, anche alla luce di alcuni significativi attacchi

hacker (ad esempio WannaCry, che ha colpito nel 2017 i PC delle strutture ospedaliere britanniche) volgendo così lo sguardo alla sicurezza informatica come al principale asset da salvaguardare, in Italia, nel 2019, per paralizzare il traffico ferroviario dell'alta velocità, e quindi il paese, è sufficiente appiccare un incendio nell'area dove si trovano i cavi di trasmissione dati degli apparati di sicurezza dei treni, come è successo il 23 luglio.

I media e gli esperti della security si prodigano in scuse ma forse, l'unica vero aspetto su cui riflettere è che la convinzione che il cybercrime sia il nuovo e unico nemico, ha causato un generale abbassamento della guardia di fronte alle minacce che arrivano nel più classico dei modi, quello fisico. Abbiamo forse perso tutti la consapevolezza, (o possiamo pensare che in taluni casi la consapevolezza non ci sia mai stata?) che i rischi e le minacce possono ancora interessare la sicurezza in senso fisico?

Riprendendo, infatti, le parole usate a rivendicazione dell'attacco che sostengono come «sia sufficiente accendersi una sigaretta all'aria aperta […] per mandare in tilt questo gigante chiamato Potere che ha sempre e comunque i piedi di argilla. Come tutta la sua esaltata magnificenza, tutta la sua invincibilità, dipendano da fragili cavi disseminati un po' dovunque. Talmente vulnerabili da poter essere neutralizzati persino da una lumaca».

Tralasciando – e dissociandosi – dai toni usati dal sito su cui la rivendicazione è apparsa, è importante riportare il concetto di fallibilità e vulnerabilità di fronte ad una "semplice" azione come può essere quella di appiccare un incendio. In questo senso si è parlato di "strategia della lumaca", in riferimento al caso accaduto in Giappone nel maggio scorso, quando una lumaca, dopo essersi infilata in una centralina elettrica di una stazione, aveva causato con la propria bava un cortocircuito e la sospensione del traffico a rotaie nel sud del paese.

In realtà il coinvolgimento del movimento anarco-insurrezionalista in azioni o tentativi di sabotaggio era già

stato documentato in passato: solo nel novembre 2015 nei pressi di Bologna erano stati incendiati i cavi elettrici dell'alta velocità. Tuttavia, nonostante le precedenti minacce nessuna contromisura era stata presa allo scopo di prevenire altri attacchi simili. Si ricordi come tra gli obiettivi sensibili per i gruppi di anarchici da tempo c'è la tratta dell'Alta Velocità, contro cui sono state dirette "azioni delittuose" (La Notizia – Giornale.it) eppure uno snodo cruciale come quello di Firenze non era protetto, né controllato, e molti altri sono nelle stesse condizioni. È lo stesso direttore Moretti ad ammettere come il nodo di Firenze, nonostante fosse un punto fondamentale e strategico per la gestione della circolazione dei treni, non era adeguatamente sorvegliato.

L'attenzione generale della comunicazione nazionale è, dunque, sempre più orientata al pericolo degli attacchi informatici, al 5G, alla cyberguerra, all'intelligenza artificiale, e verso tutte le nuove tecnologie con le quali è giusto e fondamentale cercare di tenere il passo e rimanere aggiornati, mentre, però, il paese si ferma perché neppure il dysaster recovery e la business continuity sono di fatto concretizzati nei modelli di security dei grandi player che condizionano il sistema paese.

In virtù di queste considerazioni è imprescindibile ricordarsi che non possiamo smettere di fare analisi e assessment che ci possano dare un quadro completo e concreto dei possibili rischi e "banalmente" intraprendere misure fisiche, mutuate dalla sicurezza tradizionale, come sensori e telecamere, che se parte di un piano strategico di security complessivo e se installate, programmate, monitorate e mantenute secondo logiche innovative, ed in luoghi chiave e strategici, possano aiutarci a difendere e proteggere in maniera reale, seppur mai assoluta, gli asset pubblici di questo paese come quelli privati di aziende ed organizzazioni.