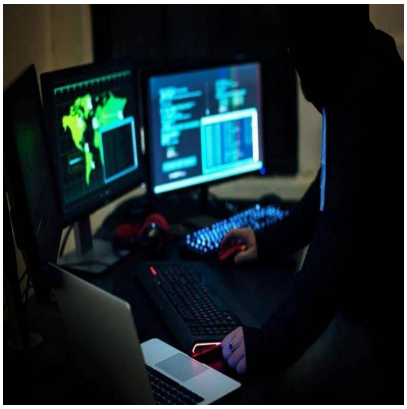


Allarmi bomba, lâ??analista German Marshall Fund: â??Lâ??Europa Ã¨ nellâ??era della guerra ombraâ?•

Descrizione

default watermark

(Adnkronos) â?? Il panico che per qualche ora ha paralizzato seimila scuole in Italia, le allerte che hanno scosso i principali scali aeroportuali di Francia, del Regno Unito e della stessa penisola italiana, e le tensioni crescenti che attraversano i confini comunitari non sono episodi isolati, ma tasselli di un mosaico molto piÃ¹ complesso. A fare il punto su questa fase di forte instabilitÃ in unâ??intervista allâ??Adnkronos Ã¨ Heli Tiirmaa-Klaar, esperta tecnologica del German Marshall Fund, il think tank di Washington Dc specializzato nel rafforzare la cooperazione in materia di sicurezza e di sfide geopolitiche tra Europa e Usa. Secondo lâ??analista estone, lâ??Europa si trova nellâ??era della â??guerra ombraâ?•. â??Prima di tutto, le autoritÃ devono stabilire chi câ??Ã¨ dietro queste minacce. Se si trattasse di un attore statale, sarebbe davvero preoccupante. Sarebbe una componente importante di questa guerra ombra. Ma se fosse un gruppo criminale, o magari solo una bravata, allora sarebbe tutta unâ??altra storiaâ?•, afferma Tiirmaa-Klaar.

Nelle ultime settimane, il ripetersi di falsi allarmi bomba e di azioni di disturbo ha messo a dura prova i nervi dei cittadini e la macchina dei soccorsi. Episodi come quello delle migliaia di istituti scolastici italiani messi in subbuglio da e-mail di spam, poi, rivelatesi provenire da un account di Taiwan, dimostrano quanto sia estremamente facile generare il caos sfruttando i canali digitali. Ciononostante, la linea di demarcazione tra una bravata giovanile, unâ??azione della criminalitÃ organizzata e unâ??operazione di ingegneria sociale, orchestrata da uno Stato estero, resta sottile ma fondamentale. â??Ricordate gli attacchi informatici contro i supermercati francesi e altri, che si Ã¨ scoperto provenire dallâ??Iran? Come vedete, in questi casi attribuire la responsabilitÃ Ã¨ molto importante. Non possiamo fare supposizioni prima di sapere chi Ã¨ stato. Ã? difficile dire come dovremmo rispondere, ma di certo gli europei devono diventare piÃ¹ resilientiâ?•, ribadisce lâ??esperta, sottolineando come la risposta politica e diplomatica dipenda in modo cruciale dalla certezza delle prove. Mentre lâ??Europa guarda con apprensione alle proprie vulnerabilitÃ , la prospettiva dâ??Oltreoceano offre una chiave di lettura diversa. Il caos registrato negli aeroporti americani questo venerdÃ¬ ha fatto temere il peggio, facendo subito pensare a un cyberattacco su larga scala. Si Ã¨ trattato, in realtÃ , di un inconveniente tecnico, legato a un aggiornamento tecnologico per il passaggio dallâ??uso di cavi in rame a quelli in

fibra ottica.

Allo stesso tempo, secondo lâ??analista del German Marshall Fund, sul fronte della sicurezza informatica pura, la posizione statunitense appare solida: â??In genere, gli Stati Uniti sono piuttosto avanzati in materia di resilienza informatica: le organizzazioni, soprattutto nel settore dei trasporti e degli aeroporti, utilizzano le tecnologie piÃ¹ avanzate e molte aziende informatiche americane sono molto solide. Non sono particolarmente preoccupata per gli attacchi informatici alle infrastrutture critiche negli Stati Uniti, perchÃ© gli esperti informatici sanno cosa fare e come costruire la resilienzaâ?•. Tuttavia, lâ??esperta mette in guardia contro ogni eccesso di ottimismo: la perfezione non esiste. Rimane sempre margine dâ??azione per un aggressore altamente qualificato in grado di sfruttare falle complesse per provocare interruzioni sistemiche.

Nel Vecchio Continente, il quadro normativo ha compiuto passi da gigante, in particolare grazie allâ??adozione della direttiva Nis (Network and Information Security), ormai recepita da tutti i Paesi membri. Questo scudo legislativo garantisce che le infrastrutture di primaria importanza dispongano di standard di protezione di base adeguati. â??Questo non significa che la sicurezza sia al cento per cento. Rimane sempre la possibilitÃ che un aggressore molto esperto riesca a penetrare le difese e, con metodi di attacco sofisticati e avanzati, provochi il caosâ?•.

default watermark

Il vero tallone dâ??Achille, di fatto, non risiede nei grandi centri di controllo, ma nei dispositivi periferici, apparentemente marginali, connessi alla rete. â??Quello che abbiamo visto con i frigoriferi dei supermercati in Europa potrebbe essere un esempio di uno di quegli anelli deboli che sono stati attaccatiâ?•, osserva Tiirmaa-Klaar. â??I frigoriferi non fanno parte delle infrastrutture critiche, ma sono apparecchiature connesse a Internet e poco sicure. Questo Ã¨ uno degli anelli deboli che abbiamo. Il problema, in Europa, Ã¨ che non dovremmo avere anelli deboli di questo tipo: dovremmo proteggere anche tutti questi punti vulnerabiliâ?•.

La sfida per il futuro non risiede soltanto nellâ??approvare nuove leggi â?? spiega Tiirmaa-Klaar â?? ma nellâ??assicurare che i singoli Stati applichino rigorosamente le norme esistenti, estendendo i requisiti di sicurezza anche al settore privato. Di fronte a scuole evacuate, aeroporti bloccati e titoli allarmistici, la reazione emotiva del pubblico oscilla spesso tra lo smarrimento e la paura. Il consiglio degli esperti di fronte a questa ondata di minacce ibride Ã¨ netto: â??Il consiglio migliore Ã¨ mantenere la calma e andare avanti, perchÃ© le minacce sono rimaste tali: non Ã¨ successo nulla, giusto? Ã? comunque molto, molto preoccupante che siano state fatteâ?•. La resilienza, in ultima analisi, non Ã¨ solo una questione di firewall, crittografia e protocolli di emergenza per le infrastrutture critiche, ma passa anche attraverso la maturitÃ collettiva di una societÃ capace di non cedere al panico, pretendendo al contempo risposte rapide e trasparenti da parte delle istituzioni. â??Abbiamo giÃ una normativa. Ora spetta ai singoli Paesi europei assicurarsi di attuarla e di imporre standard e requisiti anche al settore privato, affinchÃ© tutte le organizzazioni si occupino della sicurezza informaticaâ?•, conclude Tiirmaa-Klaar. (di Iacopo Luzi)

â??

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 14, 2026
Autore
redazione

default watermark