Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani Piano Nazionale di Ripresa e Resilienza | Tor Vergata Università degli Studi di Roma

# L'interrelazione pubblico-privato nella funzione di cybersicurezza

Il Progetto è finanziato con fondi del Ministero dell'Università e della Ricerca, PRIN Project 2022 n. ZNBAFS_001 - Settore ERC SH2

Tecnologie come lo SPID, le email, i social media, il cloud, il commercio elettronico e i servizi di pagamento via web, solo per citare quelle più utilizzate dalla popolazione, per arrivare fino agli strumenti più complessi di intelligenza artificiale, di data mining, o alla blockchain con tutte le connesse implicazioni in termini di trading online e criptovalute, rappresentano delle grandi occasioni di progresso economico - sociale, ma portano con sé altrettante problematiche (se non veri e propri pericoli), in termini di compatibilità con l'attuale assetto delle regole, di effetti sulla società civile e sul suo equilibrio economico e, in particolare, di esposizione ai tentativi di attacchi informatico malevolo.
La minaccia cibernetica è trasversale e altamente pervasiva, può colpire ovunque e indistintamente i cittadini, il settore pubblico o quello privato e sfruttare le interazioni negative che ne derivano "a cascata" in un sistema di informazioni e servizi, quale quello globale, diffusamente interconnesso.
Per contrastarla, anche l'attività di prevenzione e di difesa - in caso di attacco informatico - deve essere organizzata a livello di sistema, attraverso una rete di protezione che veda collaborare le istituzioni insieme alle imprese, in particolare quelle che operano in settori considerati più sensibili ovvero essenziali per lo Stato come la difesa, le tecnologie digitali più innovative, i servizi di pagamento, la supply chain. La recente istituzione dell'Agenzia nazionale per la cybersicurezza e del PSNC – Perimetro di sicurezza nazionale cibernetica vanno proprio in questo senso: centralizzare la risposta alle cyberminacce e costituire una infrastruttura di partenariato pubblico - privato dedicata ad assicurare una zona di spazio digitale sicuro per il funzionamento dei servizi essenziali del Paese e per il monitoraggio congiunto verso possibili minacce informatiche.
La recente cronaca internazionale, quando riporta i fatti del conflitto tra Ucraina e Russia, non manca mai di sottolineare che non si tratta più soltanto di una guerra d'invasione territoriale, ma anche di una guerra che si combatte sulla Rete, a colpi di fake news e di propaganda, e nella Rete, attraverso attacchi informatici e cyberspionaggio che mirano a paralizzare l'operatività digitale del proprio avversario. La gravità del conflitto, e il sistema di sanzioni applicato dai Paesi Nato alla Russia, espone questi ultimi a potenziali ritorsioni. Proprio nel tentativo di proteggere il sistema nazionale da queste minacce, il governo italiano ha di recente messo al bando l'utilizzo del diffuso software antivirus di produzione russa Kaspersky (installato sui computer di circa 2200 enti pubblici, tra cui i Ministeri degli interni, degli esteri e della difesa), sebbene motivando ufficialmente di voler evitare i prevedibili ritardi nello sviluppo degli aggiornamenti software e nella fornitura del servizio antivirus dovuti allo stato di guerra. Per altro verso, sempre dalla vicenda russo – ucraina scaturisce la recente allerta dell'Easa – European Aviation Safety Agency sulla sicurezza dei voli in Europa, a causa dei malfunzionamenti del sistema informatico di posizionamento satellitare Gnss dovuti ai reciproci tentativi di aggressione cibernetica in atto nelle zona del conflitto, i cui effetti si estendono a tutto il Mediterraneo orientale e incidono così sulla circolazione dell'utenza, sulla sua sicurezza e sull'attività economica delle compagnie aeree.

Per queste evidenze diviene essenziale approfondire alcuni quesiti: con quali modalità, e con quanta intensità, il rapporto pubblico - privato viene inciso dal rischio di minaccia cibernetica? In cosa consiste la reazione dello Stato, e quella dei privati, a simili eventi? In tutto questo, quale è il ruolo dell'Europa e quali sono gli strumenti da questa messi in atto?

PI: Prof. Riccardo Ursi Università degli studi di Palermo
Responsabile Unità Università degli studi di Roma Tor Vergata: Prof. Marco Macchia