PRIMO PIANO Il Sole 24 Ore 03 LUGLIO 2024

Incursioni hacker in aumento del 56% L'ipotesi spionaggio

I.Cimm.

ROMA

Nei primi cinque mesi del 2024 gli eventi di cybercrimine sono aumentati di oltre il 56% in confronto con lo stesso periodo del 2023. Non solo, rispetto ai dati di maggio dell'anno scorso, le incursioni verso infrastrutture strategiche sono lievitate del 106% (si veda il grafico a sinistra).

I dati dell'Agenzia per la cybersicurezza nazionale (Acn), organismo della presidenza del Consiglio diretto dal prefetto Bruno Frattasi, confermano la minaccia di carattere internazionale.

Un tema che va oltre le azioni dei collettivi hacker indipendenti — anche se sponsorizzati da Russia, Cina e Corea del Nord — cui sono da attribuire le massive operazioni di hacktivismo (o cyber attivismo), come il blocco dimostrativo dei portali web di Pubbliche amministrazioni e imprese private (attacchi DDoS). Secondo la relazione annuale della nostra intelligence, infatti, il ricorso a questi collettivi «esterni» e a questo tipo di attacchi ha uno scopo: consentire ai reparti militari che si occupano della guerra cyber di concentrarsi su obiettivi strategici di più alto livello, ottenendo, al contempo, un «ulteriore strato di anonimizzazione» per scansare l'attribuzione diretta di queste azioni.

La conferma è arrivata nel 2023. L'acutizzarsi delle tensioni geopolitiche — relative sia al perdurare della guerra tra Russia e Ucraina sia al mutamento degli equilibri in Medio Oriente — ha visto l'ascesa del fenomeno dell'hacktivismo con le azioni DDoS. Rispetto al 2022, infatti, questo tipo di attacchi è schizzato del 625%. Gli 007 confermano che questo aumento può indicare che alle spalle dell'hacktivismo si muovano organismi militari con l'obiettivo di portare a termine operazioni di cyberspionaggio più sofisticate. Si pensi, inoltre, che dal monitoraggio delle piattaforme utilizzate dai collettivi hacker per la rivendicazione degli attacchi DDoS, è stato rilevato che l'Italia è il sesto Paese al mondo più interessato, mentre è il terzo tra i Paesi dell'Unione europea (si veda il grafico a sinistra).

Contro il DDoS, i Csirt (squadre italiane di risposta agli incidenti di sicurezza informatica), istituiti all'interno dell'Agenzia per la cybersicurezza nazionale, nel 2023 hanno compiuto campagne di allerta per i soggetti obiettivo, indicando contromisure di mitigazione specifiche per gli attacchi in corso, oltre a pubblicare sul portale pubblico bollettini dedicati. Inoltre, sono proseguite le attività di sensibilizzazione, avviate già dal 2022, al fine di elevare il livello di allerta degli operatori pubblici e privati sui

potenziali "contagi" degli attacchi, in particolare per quelle realtà che condividono reti e sistemi.

Ma torniamo al bilancio dell'Acn. Stando al report di maggio, gli eventi cyber principali hanno riguardato la Pubblica amministrazione centrale (72), i trasporti (40), le telecomunicazioni (30), il settore tecnologico (18), l'aerospazio (14), i servizi finanziari (13), il manifatturiero (13), l'energia (11) e altri comparti (52) (si veda il grafico in basso).

«Le politiche di cybersicurezza sono diventate prioritarie in un periodo di crescenti attacchi informatici e la partnership pubblico-privato è importante, le istituzioni da sole non possono farcela». Lo ha detto il direttore dell'Agenzia Frattasi, intervenendo ieri alla Conferenza internazionale per la costruzione di un ecosistema di cyber capacity building svolto alla Farnesina.

Secondo il vicepremier e ministro degli Esteri Antonio Tajani, «di fronte alle crescenti minacce alla nostra sicurezza in ambito cibernetico, il Governo è fortemente impegnato in un'azione volta a rafforzare la sinergia tra enti pubblici e privati, mondo accademico e centri-studio».

Per il ministro dell'Interno Matteo Piantedosi «serve un'adeguata protezione dagli attacchi: si pensi alla tempesta di disinformazione che si scatena durante gli appuntamenti elettorali, o ai massicci attacchi ad ospedali ed aziende di trasporti. Sono azioni che possono paralizzare settori importanti di un Paese. Lo sviluppo di un expertise in materia è dunque un elemento vitale».