ItaliaOggi Sette

21-NOV-2022
pagina 17 /
foglio 1 / 2

I dati del nuovo rapporto Clusit sulle incursioni in rete: colpite società, politica, economia

Cyber criminalità a tutto campo

Attacchi su dell'8,4%. Più di un quarto colpisce l'Europa

DI ANTONIO LONGO

Nei primi sei mesi del 2022 sono stati 1.141 gli attacchi cyber gravi, ossia che hanno avuto un impatto sistemico in diversi aspetti della società, della politica, dell'economia e della geopolitica, con una crescita dell'8,4% rispetto al primo semestre 2021, per una media complessiva di 190 attacchi al mese, con un picco di 225 attacchi a marzo 2022, il valore più alto mai verificato. A certificarlo la nuova edizione del rapporto Clusit 2022 sulla sicurezza cyber.

I ricercatori di Clusit hanno identificato, classificato e valutato dal 2011, data della prima pubblicazione del rapporto, ad oggi oltre 15 mila attacchi informatici gravi, di questi più della metà (8.285) si sono verificati negli ultimi 4 anni e mezzo, a causa di un'accelerazione delle minacce cibernetiche. Se confrontati con il primo semestre 2018, gli attacchi da gennaio a giugno 2022 hanno fatto registrare una crescita del 53%. In quattro anni e mezzo la media mensile di attacchi gravi a livello globale è passata da 124 a 190.«L'Italia deve cogliere l'opportunità della transizione digitale per colmare le proprie lacune in materia di sicurezza informatica» osserva **Gabriele Faggioli**, presidente di Clusit, «lo scenario geopolitico ci pone con brutalità davanti all'obbligo di avere infrastrutture resistenti ad attacchi esterni che potrebbero minare la capacità di erogare servizi essenziali ai cittadini. Credo che mai come ora sia fondamentale una scelta politica forte e possibilmente univoca a livello europeo; mai come ora è importante usare al meglio le risorse del Pnrr, nel contesto di uno sforzo politico e imprenditoriale collettivo che servirà per superare l'attuale crisi e per affrontare le prossime sfide».

Attacchi sempre più dannosi. A giudizio degli analisti, il trend di crescita degli attacchi riguarda anche la "qualità" degli stessi che agisce da moltiplicatore dei danni. Confermando una tendenza già evidente nel 2021, gli attacchi gravi con effetti molto importanti sono stati nel primo semestre 2022 il 45% del totale, mentre quelli con impatto "critico" arrivano nei primi sei mesi di quest'anno a rappresentare un terzo di tutti gli attacchi. Nel complesso, gli attacchi con impatto "critical" e "high" sono stati il 78% del totale. «Siamo sulla soglia di una guerra cibernetica globale» precisa **Andrea Zapparoli Manzoni**, coautore del rapporto e membro del comitato direttivo dell'associazione, «d'ora in poi le infrastrutture critiche e molti altri sistemi digitali, meno tutelati a livello normativo ma comunque essenziali per la collettività, saranno bersagli designati, costantemente al centro del mirino di numerosi attori, governativi e non».

I settori più attaccati. Tenendo come base di raffronto il primo semestre 2021, nel primo semestre 2022 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "multiple targets" (+108,3%), significa, secondo gli autori del rapporto, che i cyber criminali tendono a colpire in maniera indifferenziata obiettivi molteplici, piuttosto che bersagli specifici. Tale crescita a tre cifre porta la categoria in testa alla classifica delle vittime anche in termini percentuali, rappresentando il 22% del totale. In termini di crescita percentuale seguono le categorie "telecomunicazioni" (+77,8%), "finanziario/assicurativo" (+76,7%), "notizie /multimedia" (+50%), "manifatturiero" (+34%), "altri servizi" (+30,8%) ed "Ict" (+11,5%), "energia / utilities" (+5,3%) e "salute" (+2,2%).

Il conflitto russo-ucraino. Il primo semestre 2022 ha registrato un'impennata del 414% delle attività riferibili agli attacchi della categoria "hacktivism"; quelli relativi all'"information warfare" sono cresciuti del 119%.

Tali incrementi a tre cifre vanno ricondotti, secondo i ricercatori di Clusit, in primo luogo alla guerra in Ucraina. Per la stessa motivazione, rispetto al primo semestre del 2021, sono aumentate del 62% rispetto allo stesso periodo del 2021 degli attacchi con finalità di "spionaggio". Dopo il picco straordinario del 2021, nel primo semestre 2022 sono, invece, diminuiti del 3,4% gli attacchi classificati come attività di "cybercrime" che rimane, tuttavia, la principale motivazione di attacco a livello globale, rappresentando il 78,4% degli attacchi globali. «Il conflitto tra Russia e Ucraina ha messo in campo strumenti cyber-offensivi altamente sofisticati a supporto di attività di cyber-intelligence e di cyber-warfare: temiamo che questo processo sia difficilmente reversibile e che in prospettiva potrebbe causare conseguenze di inaudita gravità», commenta **Sofia Scozzari**, coautrice del rapporto e membro del comitato scientifico di Clusit.

La distribuzione geografica delle vittime. Sono aumentati nel 2022 gli attacchi verso realtà basate in Europa, che raggiungono il valore più alto di sempre, con il 26% degli attacchi complessivi (in crescita dal 21% del 2021). Contestualmente, diminuiscono per la prima volta dal 2011 le vittime di area americana (dal 45% al 38%) e scendono anche quelli rilevati contro organizzazioni asiatiche (dal 12% all'8%). Inoltre, nel primo semestre di quest'anno hanno prevalso in maniera assoluta gli attacchi perpetrati attraverso "malware" che, pur registrando una leggera flessione dal primo semestre 2021(-4,6%), rappresenta il 38% del totale. Le tecniche sconosciute sono al secondo posto, con un aumento del 10% rispetto al primo semestre 2021, superando la categoria "vulnerabilità" (-26,8%) e "phishing / social engineering" che però crescono del 63,8%. In conseguenza della natura sempre più complessa degli attacchi, la categoria "Tecniche Multiple" sale del +93,8%.

Regole Ue più stringenti per la gestione dei rischi

03374

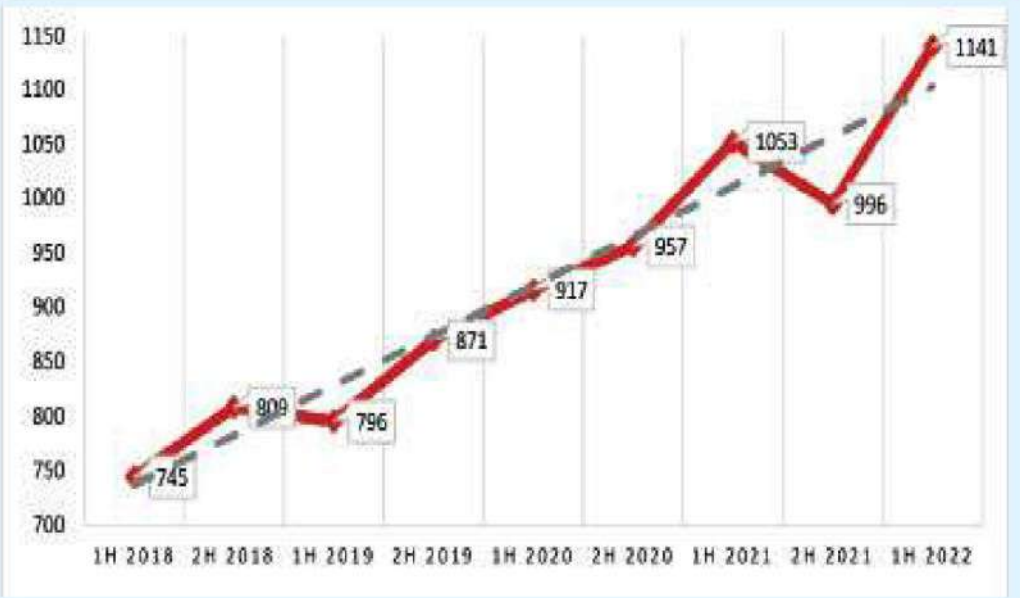
Requisiti più stringenti per imprese, amministrazioni e infrastrutture europee in materia di sicurezza informatica. Sono quelli previsti dalla nuova direttiva comunitaria Nis2, approvata nei giorni scorsi dal parlamento di Bruxelles e che dovrà essere adottata anche dal Consiglio prima che venga pubblicata nella *Gazzetta Ufficiale dell'Ue* ed entri, così, in vigore. Il nuovo provvedimento abroga la precedente direttiva sulla sicurezza delle reti e dell'informazione (Nis), primo atto legislativo a livello europeo sulla sicurezza informatica, adottato con l'obiettivo specifico di raggiungere un elevato livello comune di sicurezza informatica in tutti gli stati membri, che ha aumentato le capacità degli stessi in materia di sicurezza informatica ma la cui attuazione si è rivelata difficile.

In particolare, le nuove norme impongono ai paesi membri di adottare misure di vigilanza e di applicazione più severe, per quanto riguarda la gestione del rischio, gli obblighi di segnalazione e la condivisione delle informazioni, e di armonizzare le sanzioni, con particolare riferimento ai nuovi settori ritenuti "essenziali" come l'energia, i trasporti, le banche, la sanità, le infrastrutture digitali, la pubblica amministrazione lo spazio.

Ma le nuove norme proteggeranno anche i settori definiti "importanti" quali servizi postali, gestione dei rifiuti, prodotti chimici, alimenti, produzione di dispositivi medici, elettronica, macchinari, veicoli a motore e fornitori di servizi digitali. I requisiti riguardano, in dettaglio, la risposta agli incidenti, la sicurezza della catena di approvvigionamento, la crittografia e la divulgazione delle vulnerabilità.

Il testo della nuova direttiva stabilisce, inoltre, un quadro chiaro per una migliore cooperazione e condivisione delle informazioni tra le diverse autorità e gli stati, creando una banca dati europea. «Il ransomware e le altre minacce informatiche hanno predato l'Europa per troppo tempo, dobbiamo agire per rendere le nostre imprese, i nostri governi e la nostra società più resistenti alle operazioni informatiche ostili» ha dichiarato il relatore Bart Groothuis, «questa direttiva europea aiuterà circa 160 mila enti a rafforzare la propria sicurezza e a rendere l'Europa un luogo sicuro in cui vivere e lavorare. Inoltre, consentirà di condividere le informazioni con il settore privato e con i partner di tutto il mondo».

Gli attacchi informatici*



*Attacchi per semestre
Fonte: Clusit, Rapporto 2022 sulla sicurezza Ict in Italia – Aggiornamento giugno 2022