

L'Agenzia per la Cybersicurezza

DS1948

DS1948

Hacker contro Pa e imprese “Nel 2023 un attacco al giorno”

Relazione alle Camera:
le guerre muovono
attivisti web, a rischio
le elezioni europee
di Aldo Fontanarosa

ROMA – Nell'era dell'intelligenza artificiale, mentre due guerre si consumano tra Ucraina e Medio Oriente, l'Italia accusa attacchi hacker sempre più continui (durante il 2023), ai danni anche delle imprese. Nella Relazione annuale al Parlamento, l'Agenzia per la Cybersicurezza spiega che gli incidenti erano stati 126 nel 2022, invece l'anno scorso sono lievitati a quota 303. Quasi uno al giorno.

E in questo clima Bruno Frattasi, direttore generale dell'Agenzia, mette in guardia dai rischi anche per le prossime europee. Dice, in particolare, Frattasi: parliamo «con il ministro Piantedosi (Interni) per sensibilizzare le postazioni elettorali sull'uso dei sistemi digitali per la raccolta dei risultati». Più in generale, Lorenzo Guerini - presidente del Comitato parlamentare per la sicu-

rezza della Repubblica (Copasir) - invita l'opinione pubblica a vigilare su una forma assai subdola di inquinamento del voto via web: le notizie false, le bufale.

Ben 303 incidenti nel solo 2023, dunque. L'Agenzia, nostra massima sentinella in questo campo, spiega che l'incidente è «un evento cyber» che impatta «sull'integrità delle informazioni». Un evento dannoso, che va a segno. Se consideriamo gli eventi che hanno fallito l'obiettivo, allora il numero totale sale a 1.411. Aumentano anche i soggetti bersaglio di questi assalti: erano 1150, sono diventati 3302. Ora, sarebbe ingenuo pensare a un esercizio da “smattoni” che si consuma sopra le nostre teste. Al contrario, i pirati informatici puntano ai cuori vitali di una Nazione: alle aziende di Internet, alle infrastrutture dell'energia, ai trasporti, agli uffici pubblici (centrali e locali), a volte ad ospedali, Asl, università.

Le guerre del mondo motivano gli hacker a muoversi. L'Agenzia per la Cybersicurezza conta 319 eventi DDoS, tipici degli attivisti del web che paralizzano siti soprattutto pub-

blici, ad esempio con un bombardamento di email. In alcuni casi, le pagine normali dei siti sono rimpiazzate da altre che contengono «apologia e rivendicazioni». I «collettivi filorussi» sono i più determinati, con 248 assalti all'attivo; mentre lo stesso gruppo filopalestinese ha condotto una campagna con 15 attacchi. Dati che inquietano Alfredo Mantovano, sottosegretario alla Presidenza del Consiglio.

L'odiosa pratica dei ricatti - ti liberiamo il sito se ci paghi - intanto tormenta il nostro Paese, il terzo più colpito dell'Ue (dopo Germania e Francia). Ovviamente l'Agenzia non si limita a fotografare, inerme, gli assalitori. Suo compito è organizzare difese sempre più alte e sofisticate. Nel 2023, una squadra di suoi specialisti ha raggiunto le imprese o le strutture pubbliche aggredite in 13 casi, per assisterle sul campo. In altri 38 casi, l'aiuto è stato assicurato da remoto. Importante è che la Pubblica Amministrazione acquisti hardware e software adeguati al contesto. Per questo il Codice dei contratti pubblici dà ora indicazioni vincolanti al riguardo.

© RIPRODUZIONE RISERVATA



Enti pubblici

A dicembre 2023, hacker russi colpiscono i servizi cloud della società Westpole. Oltre mille enti pubblici, che si appoggiavano a loro, accusano disservizi

Ospedale

A luglio 2023 pirati informatici colpiscono l'ospedale Vanvitelli di Napoli. Molti file della struttura sono criptati e resi inservibili. L'Agenzia interviene

