

Source: L'edicola Del Sud - Bari Author:
Country: Italy Date: 2025/06/19
Media: Printed Pages: 10 - 10

Gross Reach: 15.000
Gross Pr Value: € 750
Pages Occupied 0.5



L'ALLARME

Cyber-attacchi, ogni mese 165 episodi Indispensabile formare nuovi esperti

Quello visto nel 2024 è un trend in crescita che non risparmia nessuno: cittadini, imprese e istituzioni. Proprio per questo motivo serve creare altri "difensori" e figure di riferimento attraverso corsi di studi nelle università incentrati sulle materie Stem

FABIO PENGO

ROMA

La criminalità informatica non solo è cresciuta, ma si è strutturata, diventando transnazionale, sofisticata e redditizia. È il messaggio che arriva dall'Agenzia per la Cybersecurity Nazionale (Acn), che ha presentato i dati allarmanti del 2024 durante l'evento Cybersecurity Seminars, tenutosi al Campidoglio di Roma.

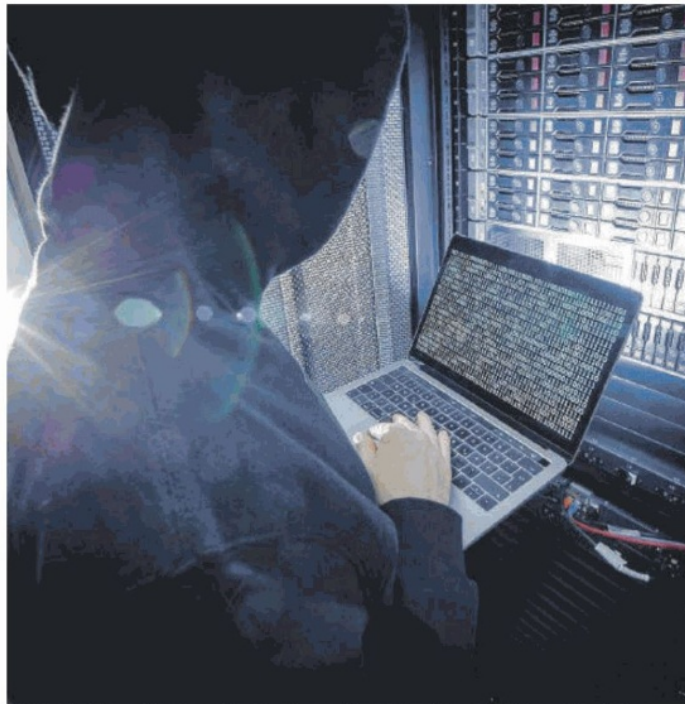
I dati

Il quadro è netto: 165 attacchi informatici al mese, per un totale di 2.734 vittime, il doppio rispetto all'anno precedente. I numeri testimoniano una minaccia ormai sistemica, che non risparmia nessuno: dalla sanità ai trasporti, dalle piccole imprese agli enti pubblici. A guidare la classifica delle tecniche più diffuse ci sono gli attacchi ransomware, veri e propri sequestri digitali con richiesta di riscatto, che colpiscono in modo crescente soprattutto le piccole e medie imprese, spesso senza adeguate difese. Ad affrontare il nodo di una risposta

efficace è stata la vicedirettrice generale di Acn, Nunzia Ciardi, intervenuta nel corso della presentazione di un progetto sostenuto da Google.org in collaborazione con Virtual Routes, l'Università degli Studi di Milano e la Fondazione Mondo Digitale. «La criminalità informatica è difficile da contrastare e altamente redditizia - ha spiegato Ciardi - serve una resilienza condivisa tra i Paesi avanzati, perché ci troviamo davanti a una minaccia pervasiva che investe tutti i servizi essenziali».

Il piano di difesa

Al centro dell'iniziativa c'è un investimento chiaro nella formazione: costruire nuove competenze, rafforzare la cultura della sicurezza digitale e creare una rete di esperti in grado di affrontare le sfide del cybercrime. La chiave è quindi il capitale umano, non solo quello altamente tecnico, ma anche trasversale e multidisciplinare. Cybersecurity Seminars ha già ottenuto risultati incoraggianti: il programma ha attratto partecipanti da oltre 40 classi di laurea, in



L'attacco hacker più frequente è il ransomware: si tratta di qualcuno che si impossessa di dati sensibili di qualcun altro per poi riconsegnarglieli sotto pagamento

Contro ogni aspettativa il 30% di allievi aspiranti hacker etici è fatto di ragazze

rappresentanza di più di 40 atenei italiani. Un dato significativo è la presenza femminile: il 30% degli iscritti sono donne, una percentuale superiore alla media nei settori STEM. «L'obiettivo - ha spiegato Mirta Michilli, direttrice generale della Fondazione Mondo Digitale - è trasformare studentesse e studenti di ogni facoltà in protagonisti del cambiamento, offrendo esperienze formative concrete, interdisciplinari e orientate all'impatto sociale». In un contesto dove la minaccia digitale è in continua evoluzione, il futuro della cybersecurity italiana passa dunque dalla formazione e dalla consapevolezza. Perché il primo vero scudo contro il crimine informatico resta l'essere umano, purché sia preparato.