VareseNews

Cybersecurity, un attacco ogni 21 secondi: la nuova mappa del rischio passa da Varese

Pubblicato: Lunedì 23 Marzo 2026

Non è più solo una questione tecnica, ma il cuore pulsante della resilienza di un'impresa. La sicurezza informatica nel 2025 ha tracciato una nuova frontiera, dove i confini geografici si sfumano e l'intelligenza artificiale accelera drasticamente i tempi del cybercrime. È quanto emerge dal «Data Gathering 2026», il report annuale presentato da Elmec Informatica presso il Campus di Brunello, che analizza lo stato della cybersecurity attraverso i dati di 211 aziende italiane.

I numeri: un assedio costante

I dati globali sono impressionanti: lo scorso anno sono stati rilevati oltre 678 milioni di tentativi di attacco, il che equivale a 1,86 milioni al giorno, ovvero un attacco ogni 21,5 secondi. Nello specifico del monitoraggio Elmec, sono state registrate 21.000 anomalie e 12.000 incidenti informatici, di cui 36 hanno avuto un impatto significativo sul business delle aziende coinvolte.

La sorpresa geografica: attacchi dall'Occidente

Il report scardina un vecchio pregiudizio: i Paesi emergenti e il blocco orientale non occupano più le prime posizioni per origine degli attacchi. La classifica vede ora in testa gli Stati occidentali: Irlanda (5,4%), Stati Uniti (4,5%) e Italia (2,7%).
«I gruppi criminali scelgono territori politicamente meno sospetti ma dotati di infrastrutture digitali avanzate», spiega il report. Il dato italiano è legato sia alla forte presenza di data center internazionali,

sia a strategie che sfruttano la prossimità geografica per aggirare le difese basate sulla geolocalizzazione.

IA e fattore umano: il phishing diventa «intelligente»

Il fattore umano resta l'anello debole: nei test di simulazione, il 55% di chi ha aperto una mail sospetta ha poi cliccato sul link malevolo. L'uso dell'IA generativa ha reso queste trappole micidiali, portando il tasso di successo (click-through rate) al 54%, contro il 12% delle mail scritte manualmente.
Ancora più allarmante il dato sulle credenziali: nel primo semestre 2025 i furti tramite malware sono aumentati dell'800%, arrivando a 1,8 miliardi di dati sottratti.

Le sfide del 2026: tra NIS2 e sicurezza OT

Il futuro prossimo vede le aziende impegnate su nuovi fronti:

Sicurezza OT: la protezione delle macchine di produzione è prioritaria contro hacker specializzati nel colpire i sistemi industriali.

Passwordless e Biometria: per contrastare i deepfake, si punta su autenticazioni «liveness» che richiedono espressioni facciali o modelli vocali.

Normativa NIS2: l'adeguamento legislativo viene indicato non come semplice obbligo, ma come investimento strategico.

«La sicurezza non può più essere frammentata: serve un approccio end-to-end che coniughi protezione e resilienza», ha dichiarato Filadelfio Emanuele, CISO di Elmec Informatica, durante il «Summit 30: Security», sottolineando come la collaborazione tra partner sia oggi l'unica chiave per affrontare una minaccia senza confini.

Redazione VareseNews
redazione@varesenews.it