State of Cybersecurity: Italia sotto attacco

Pubblicato il 28/08/2025

L'Italia si trova al centro di un'ondata di attacchi informatici, con un **aumento del 14%** nel primo semestre del 2025 rispetto all'anno precedente. I dati, emersi dal rapporto **State of Cybersecurity** di Aused e Certego, rivelano un'escalation di minacce che colpiscono indiscriminatamente grandi aziende, piccole e medie imprese (PMI) e il settore pubblico. Questo fenomeno trasversale sottolinea la crescente vulnerabilità del sistema economico italiano, rendendo la **sicurezza informatica** una priorità strategica per il Paese.

I settori più colpiti e le fonti degli attacchi

I dati del rapporto evidenziano chiaramente quali sono i settori più presi di mira dai cybercriminali. Il **Manufacturing/Industry** guida la classifica con ben 2.897 attacchi, registrando un aumento del **20%**. Questo dimostra come le fabbriche italiane, pilastri dell'economia, siano diventate un obiettivo primario. Subito dopo si collocano **Finance/Insurance** con 2.613 attacchi (+20%), un target logico dato il valore dei dati sensibili

e delle risorse economiche che gestiscono. Anche settori come **Fashion/Design**, **Chemical/Pharmaceutical** ed **Energy/Environment** hanno visto un incremento significativo degli attacchi, a testimonianza di una diversificazione delle minacce.

La provenienza di questi attacchi non sorprende gli esperti. La **Cina** si conferma come la principale fonte di cyber minacce, seguita da **Stati Uniti**, **Russia** e **India**. Le armi preferite dagli hacker rimangono i **malware**, il **phishing** e il **social engineering**, tecniche che sfruttano le vulnerabilità umane e tecnologiche per ottenere accesso a sistemi e dati.

Le vulnerabilità e le strategie di difesa

Gli hacker sfruttano principalmente tre varchi per infiltrarsi nei sistemi aziendali: il **cloud**, i **network** e gli **endpoint**. Questi percorsi sono difficili da proteggere completamente e spesso sono compromessi da comportamenti anomali degli utenti o accessi sospetti. Di fronte a questa crescente pressione, l'analisi di Aused sottolinea la necessità di un approccio integrato che includa **investimenti in tecnologie avanzate, processi di sicurezza robusti e formazione del personale**.

La lotta contro il cybercrime richiede una stretta **collaborazione tra settore pubblico e privato**. Le aziende devono non solo rafforzare le proprie difese interne, ma anche contribuire a un sistema di sicurezza nazionale più resiliente, basato sulla condivisione di informazioni e sull'adozione di strategie comuni per contrastare un nemico invisibile ma sempre più insidioso.

Link notizia: https://www.certego.net/it/blog/whitepaper-state-of-cybersecurity-gennaio-giugno-2025/https://www.certego.net/it/blog/whitepaper-state-of-cybersecurity-gennaio-giugno-2025/