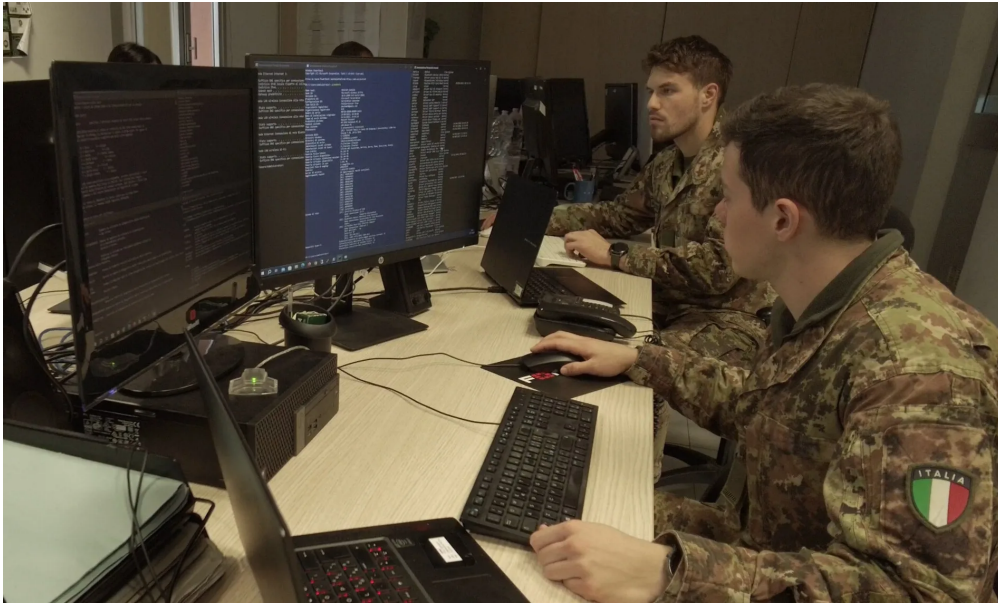




Cybersecurity e infrastrutture critiche: l'Italia al centro della guerra digitale

Pubblicato il 22/08/2025

Il settore energetico europeo, e in particolare quello italiano, è diventato uno dei principali fronti della guerra cibernetica globale. A confermarlo è il nuovo **report del Cybersecurity Competence Center di Maticmind**, che fotografa una situazione in costante peggioramento: nel 2024 gli attacchi informatici al comparto energia sono aumentati del **40% a livello mondiale**, con una previsione di ulteriore crescita del **21% per il 2025**. L'Europa, da sola, assorbe quasi il **60% degli attacchi globali**, e il nostro Paese figura tra i target più esposti.

Una minaccia alla sicurezza nazionale

La digitalizzazione delle reti elettriche e la diffusione di sistemi IoT e Scada hanno ampliato in maniera esponenziale la superficie di attacco. Ogni sensore, ogni nodo connesso può trasformarsi in una vulnerabilità sfruttabile da attori ostili. Non è un caso che gli aggressori colpiscano sia i grandi operatori sia le realtà locali, meno attrezzate a livello difensivo.

Il dato più allarmante riguarda però la natura stessa degli attacchi: **oltre il 58% degli incidenti del 2025 ha motivazioni politiche o ideologiche**. Non più solo criminalità organizzata alla ricerca di riscatto economico, ma veri e propri gruppi **hacktivisti e statuali** che utilizzano il dominio cyber come strumento di pressione strategica.

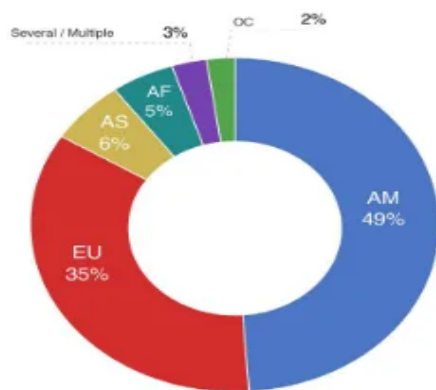


Italia, bersaglio privilegiato

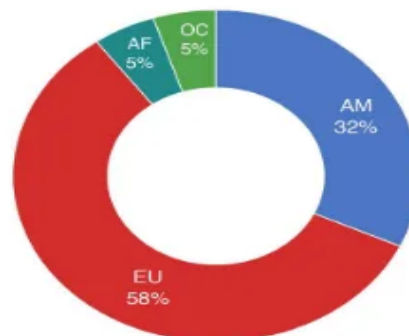
Gli episodi di **attacchi DDoS** hanno registrato un incremento del 107% nei primi mesi del 2025, mentre il **ransomware** ha fatto segnare +64% in Italia e +80% a livello globale nel biennio 2023-2024. Gruppi come **LockBit, AlphV e Qilin** hanno concentrato i propri sforzi contro le infrastrutture energetiche, attratti dall'alto valore strategico delle informazioni e dalla fragilità dei sistemi industriali.

Parallelamente, sebbene le menzioni del settore energetico sul dark web siano crollate del 75%, gli analisti segnalano che si tratta di una "ritirata apparente": la discussione si è spostata verso **forum chiusi e ambienti cifrati**, dove i riferimenti all'Italia restano altissimi.

Geografia vittime Energy/Utilities
2024



Geografia vittime Energy/Utilities
Q1 2025



EU: Europa

AS: Asia

AF: Africa

OC: Ocenia

Cybersecurity e infrastrutture critiche: l'Italia al centro della guerra digitale

Risposta europea e sfida strutturale

L'UE ha introdotto strumenti come la **direttiva NIS2**, che impone la segnalazione degli incidenti entro 72 ore e prevede sanzioni fino al 2% del fatturato. Anche il **Network Code europeo** per la sicurezza delle reti elettriche punta ad alzare il livello di protezione. Tuttavia, come evidenzia il report Maticmind, la vera criticità resta la vetustà delle infrastrutture: negli Stati Uniti, l'età media dei sistemi elettrici supera i 40 anni. Situazione simile anche in Europa, dove i sistemi legacy costituiscono una vulnerabilità difficilmente sanabile con la sola compliance normativa.

La strategia per il futuro

Gli analisti invocano un cambio radicale: non limitarsi alla difesa, ma adottare un approccio proattivo e resiliente. Le direttrici principali:

- **Zero Trust Architecture**, per ridurre il rischio interno ed esterno;
- **Threat Intelligence avanzata**, con l'integrazione di fonti Osint e feed classificati;
- **Collaborazione tra settore privato, istituzioni e Forze Armate**, in una logica di difesa integrata;
- **Digital Twin** per testare scenari complessi e simulare attacchi prima che accadano.

Come sottolinea **Pierguido Iezzi, Cyber Security Director di Maticmind**, «l'energia non è più solo produzione e consumo. È geopolitica, economia e sicurezza nazionale. Resistere non basta: bisogna anticipare e reagire con prontezza».

In uno scenario dove il confine tra conflitto convenzionale e guerra ibrida è sempre più sfumato, la protezione delle infrastrutture energetiche rappresenta una **sfida strategica per la sovranità del Paese**.

Link notizia: <https://www.maticmind.it/soluzioni-it/cyber-security>