

Anche i cyberattack minacciano il sistema energetico italiano

14 Ottobre 2022

198



Da Bureau Veritas Italia procedure e metodologia per respingere i cybercriminals

Non sono solo i tagli nei flussi di gas e le incertezze, spesso speculative, del mercato; a incombere sul futuro dell'approvvigionamento energetico dell'Italia e del suo sistema economico grava anche un ulteriore rischio, quello dei cyberattack che in modo sempre più frequente stanno prendendo di mira le aziende del settore energia, paradossalmente più esposto di quanto accadesse in passato a causa del processo di digitalizzazione delle

infrastrutture, del controllo remoto delle stesse e dello sforzo in atto verso l'affermazione di energie più sostenibili.

Secondo il Rapporto Clusit 2021 (Associazione Italiana per la Sicurezza Informatica), le imprese Energy & Utilities risultano essere tra le più colpite dai cyberattacchi, con un'impennata del 46,2% nell'ultimo anno.

In base all'analisi Swascan Energy Cyber sector 2021, l'80% delle aziende che operano nel settore energia italiano presenta ancora potenziali vulnerabilità, nonostante che (secondo il rapporto sulla Digital Maturity in Cybersecurity, realizzato da Minsait), le aziende del settore Energy si distinguano per l'implementazione di misure di Cyber Security in una filiera che vale più di 60 miliardi di euro, con oltre 3.800 imprese attive e con un numero di occupati stimato in 101 mila unità di lavoro.

Ed è su questo campo che Bureau Veritas Italia ha raccolto il guanto di sfida, mettendo a disposizione del mercato in primis un forte know-how tecnico per la valutazione del livello di sicurezza dei dispositivi connessi, garantendo un percorso di compliance rispetto alla norma IEC 62443 e su tutte le altre normative di riferimento in ambito cybersecurity.

La norma IEC 62443 richiamata direttamente all'interno del regolamento CEI – 016 è diventata un punto di riferimento al quale tutti gli operatori del settore saranno chiamati a rispondere. Obiettivo: garantire l'effettiva sicurezza degli impianti e la conseguente continuità alla fornitura di energia.

“Il cybercrime – afferma Diego D'Amato, Presidente e Amministratore Delegato di Bureau Veritas Italia – può avere impatti devastanti sulle infrastrutture essenziali e ricadute importanti sul sistema di approvvigionamento energetico del nostro Paese. Il gruppo Bureau Veritas ha già rafforzato la propria capacità di intervento su questi temi, acquisendo Secura, società specializzata in valutazioni di conformità per la cybersecurity. Siamo pronti ad agire nello scontro con questa nuova criminalità, che mira a prendere possesso di informazioni e dati incidendo profondamente sul tema, oggi caldissimo, dei flussi di energia”.