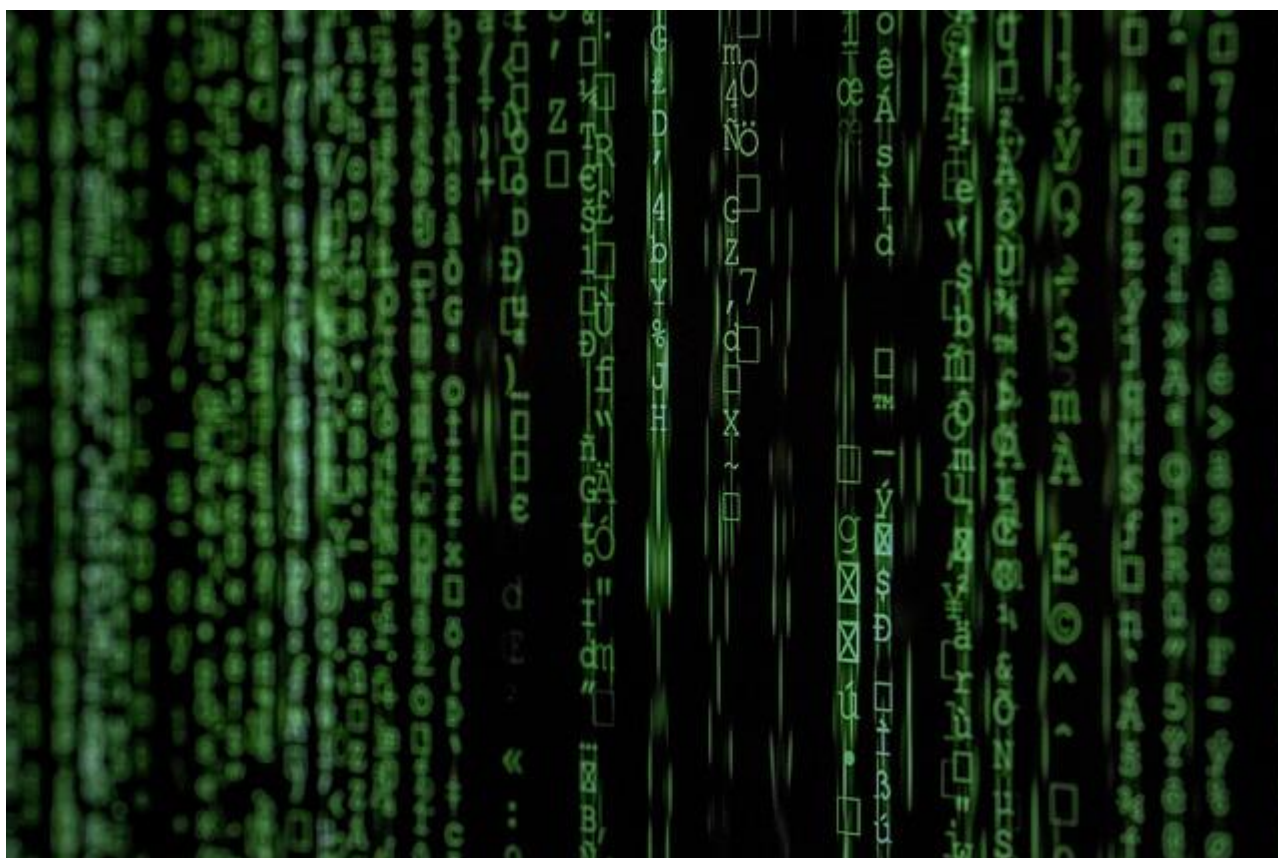


Attacchi cyber: Italia sempre più nel mirino. Come difendersi?

DI **REDAZIONE LINEA**EDP31/03/2023UPDATED:30/03/2023LETTURA 3 MIN

Secondo nuovi dati di Bureau Veritas il nostro Paese è coinvolto nel 7,6% degli attacchi globali. Riflettori accesi sul settore energia



Alla luce degli ultimi dati statistici e dei rapporti stilati da varie fonti di ricerca sembrerebbe proprio che dal 2022 “l’[Italia](#) è nel mirino” degli attaccanti in quanto subisce ormai il 7,6% degli attacchi cyber globali (contro un 3,4% del 2021). Confrontando i numeri del 2018 con quelli del 2022 la crescita del numero di attacchi rilevati è stata del 60% (da 1.554 a 2.489). Nello stesso periodo la media mensile di attacchi gravi a livello globale è passata da 130 a 207. Attacchi cyber più frequenti e con conseguenze più gravi, come testimoniato anche dalla Ricerca 2022 dell’Osservatorio Cybersecurity e Data Protection del Politecnico di Milano dalla quale emerge che il 67% delle grandi imprese ha subito un aumento dei tentativi di attacco rispetto all’anno precedente e che il 14% delle grandi imprese dichiara di aver subito attacchi con conseguenze concrete.

Secondo **Diego D'Amato**, Presidente e Amministratore Delegato di Bureau Veritas Italia, *“la cybersecurity è innanzitutto un fatto culturale: alla luce dei nuovi obblighi normativi, è indispensabile cambiare il mindset delle persone nelle organizzazioni, rivedendo comportamenti e abitudini per proteggersi dalle nuove minacce. E, chiudendo una celebre frase dell'ex direttore*

dell'FBI, è il caso di ricordare che la consapevolezza è la chiave e come si usa dire esistono solo due tipi di aziende: quelle che hanno subito un attacco hacker e quelle che non sanno di essere state attaccate. Oggi più che mai – con minacce che variano continuamente, proprio come un virus – è indispensabile valutare la propria capacità di risposta tenendo conto delle persone, dei processi e delle tecnologie: su questi tre livelli di attenzione è articolata la rosa dei servizi del gruppo Bureau Veritas”.

Nel mirino degli attacchi cyber si trova in particolare il **settore energia**, una filiera articolata 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. Ma anche una filiera su cui – in ragione della transizione verso una rete energetica digitalizzata o 4.0 – incombono sempre nuovi rischi, con nuovi accessi per gli hacker. È proprio muovendo da questi dati che **Bureau Veritas Italia** con la partecipazione di **Secura** – società del gruppo BV specializzata in cybersecurity – ha organizzato un incontro tecnico-informativo con l'obiettivo di approfondire l'evoluzione della Cybersecurity nel settore Energy e i rischi connessi a seguito di un attacco: dalla perdita di dati sensibili, all'interruzione di servizi infrastrutturali con conseguente sospensione della fornitura di energia. Un incontro ispirato al massimo pragmatismo, ovvero alla messa a punto di strategie e metodologie efficaci per combattere il rischio cyber.

Con la partecipazione dei principali Original Equipment Manufacturer, Asset owner e operatori per la trasmissione di energia del panorama italiano, l'evento si è posto il traguardo di porre a fattore comune le esperienze, anche negative, dei differenti players per condividere strategie efficaci di cybersecurity per uno dei principali settori critici, per altro condizionanti l'intero assetto economico e produttivo del sistema Paese.

Il tavolo tecnico, composto da massimi esperti Bureau Veritas Italia e della società del gruppo Secura, ha visto anche la partecipazione di importanti esponenti nazionali e internazionali sulla tematica: Il Comitato elettrotecnico Italiano chiamato ad approfondire il tema del regolamento CEI 016, Colin and Partners – società di consulenza strategica in ambito informatico – impegnata sulla direttiva NIS2 e Cyber 4.0 Centro di competenza nazionale ad alta specializzazione sulla cybersecurity, leader nelle strategie di sicurezza per una transizione digitale efficace.