Reggio Calabria, il dott. Marafioti analizza la sfida della cyber security delle reti OT

di Mirko Spadaro 31 Lug 2026 | 09:45

Il 30 luglio 2026, presso lo storico scenario del **Circolo Tennis "Rocco Polimeni"**, si è tenuto un incontro di profondo impatto sull'attuale panorama digitale: la **presentazione del libro "Cybersecurity delle reti OT. Analisi dei principali attacchi e contromisure"**, ed. **Abra Books** saggistica, del **dott. Renato S. Marafioti**. Ha introdotto i lavori l'avv. Romolo, in rappresentanza del circolo; hanno moderato i lavori la **dott.ssa Simona Malena e la dott.ssa Silvia Marra**.

L'autore, figura ponte tra le competenze tecniche ingegneristiche e quelle giuridiche, ha posto l'attenzione su una minaccia spesso sottovalutata: la vulnerabilità delle reti OT (Operational Technology). A differenza delle classiche reti IT che gestiscono dati e informazioni, le reti OT sono il "cuore pulsante" e i "muscoli" della nostra società. Esse regolano infrastrutture critiche: dalla distribuzione dell'energia elettrica al trattamento dell'acqua, fino ai sistemi di controllo dei trasporti e degli impianti industriali.

"*Attaccare l'IT significa spesso rubare dati e informazioni, attaccare l'OT significa spesso causare danni fisici reali al mondo che ci circonda*", ha spiegato Marafioti durante l'evento.

Dalle email ai blackout: una minaccia quotidiana

Marafioti ha chiarito la distinzione netta tra le minacce digitali a cui siamo abituati — come il furto di identità o la violazione di email personali — e gli attacchi alle reti OT. Se nel primo caso l'impatto è primariamente finanziario o di privacy, nel caso dell'OT l'hacker prende, metaforicamente, il controllo del volante di una società in movimento. Il libro cita casi emblematici, come il sabotaggio della centrale nucleare di Natanz nel 2010 o il massiccio attacco ransomware a Kaseya nel 2021, che ha paralizzato centinaia di supermercati in Svezia, dimostrando come le ricadute sulla quotidianità siano immediate e tangibili.

Difesa e consapevolezza: la regola d'oro

L'incontro non è stato solo un'analisi dei pericoli, ma un invito all'azione. L'autore ha delineato una strategia di difesa basata su tre pilastri: la segmentazione delle reti per isolare i sistemi critici, il monitoraggio costante del traffico di dati per identificare anomalie e la resilienza, ovvero la capacità di mantenere il controllo fisico dei sistemi anche durante un incidente.
L'incontro ha evidenziato come le reti OT (Operational Technology) rappresentino oggi un'infrastruttura critica e invisibile che governa la nostra quotidianità — dall'energia elettrica ai sistemi di trasporto. L'autore Renato S. Marafioti ha sottolineato la differenza fondamentale tra gli attacchi IT, mirati al furto di dati, e quelli alle reti OT, capaci di generare danni fisici reali. L'evento ha ribadito l'importanza cruciale della consapevolezza e della formazione continua, definendo la cultura della sicurezza come la "prima vera difesa" contro un panorama di minacce sempre più sofisticato.

In chiusura, rispondendo alla domanda sulla "regola d'oro" per la sicurezza, Marafioti ha rivolto un appello al pubblico: "*non dobbiamo pensare che la cybersecurity sia un problema solo degli altri. La tecnologia protegge, ma le persone informate proteggono di più. La cultura della sicurezza è la nostra prima vera difesa*".