EasyAudit™
KNOW THE RISK

WHITE PAPER EASYAUDIT

La sicurezza informatica e l'importanza di capire

Usare un sistema di sicurezza non ci fa comprendere automaticamente che cosa rende possibile un attacco informatico. Solo scoprire e riconoscere i punti deboli permette di difendersi in modo ottimale.

Cominciamo con un esempio concreto: un firewall può nascondere alcuni servizi, ma ad attacco avvenuto non trattiene i dati sensibili. Se i server sono aggiornati e rispondono solo a richieste SSH e HTTPS, un firewall non aggiunge molto alla difesa e può far sprecare risorse.

Tre aspetti da ricordare

- Più ci sentiamo protetti, meno ci sforziamo di capire. Troppi si affidano passivamente agli strumenti, dimenticando che per difendersi bisogna prima comprendere minaccia e avversario.
- Non sopravvalutare la difesa. Chi progetta prodotti di sicurezza reagisce più lentamente di chi cambia tecniche di attacco. La lotta è impari: un prodotto efficace costa milioni, un attacco ben preparato può richiedere pochi mesi.
- L'evoluzione degli attacchi è rapidissima. I sistemi di protezione tendono spesso a concentrarsi sul network, mentre applicazioni e dati sensibili sono quasi sempre il vero obiettivo.

Effettua un'analisi preliminare di minacce e vulnerabilità prima di acquistare strumenti: comprerai forse qualcosa, ma non è detto che sia ciò che avevi inizialmente previsto.