

Carenza di competenze nella Cybersecurity: La Risposta dell'Europa secondo ENISA

La situazione attuale
L'Europa si trova ad affrontare un grave divario di competenze nel settore della cybersecurity, con una stima che si aggira tra le 260.000 e le 500.000 figure professionali mancanti. Un numero enorme, soprattutto in un momento in cui gli attacchi informatici sono sempre più frequenti e complessi. Basti pensare che, nel 2022, gli attacchi legati alle password sono aumentati del 74%. Allo stesso tempo, tecnologie nuove come l'intelligenza artificiale e il calcolo quantistico portano con sé rischi inediti e difficili da gestire. Il problema non è solo tecnico: gli attacchi cibernetici possono bloccare servizi essenziali, danneggiare aziende e istituzioni pubbliche e mettere a rischio l'autonomia digitale e la stabilità economica dell'intero continente.

Il Quadro Europeo
Per affrontare questa emergenza, l'Agenzia europea per la cybersecurity (ENISA) ha adottato un piano strategico basato sullo *European Cybersecurity Skills Framework (ECSF)*. Si tratta di un modello che definisce in modo chiaro i 12 ruoli professionali fondamentali nel settore, come ad esempio gli esperti di risposta agli incidenti o i consulenti legali in ambito cyber. Oltre 20 Stati membri hanno già adottato l'ECSF. Grazie alla collaborazione con più di 40 università, ENISA sta allineando i percorsi accademici alle reali esigenze del mercato, colmando così il divario tra formazione e applicazione pratica. Sono inoltre attivi progetti mirati per settori particolarmente a rischio: gli ospedali ricevono formazione specifica contro i ransomware, i fornitori di energia si concentrano sulla sicurezza delle smart grid e, con l'Agenzia Spaziale Europea (ESA), si affrontano le vulnerabilità dei sistemi satellitari.

La forza lavoro della cybersecurity
Guardando al futuro, ENISA punta a un'espansione rapida e inclusiva della forza lavoro nel settore. Tra le priorità del 2024 ci sono:

- Estendere gli esercizi *Cyber Europe*, che attualmente formano oltre 1.200 professionisti l'anno;
- Introdurre obblighi di mappatura delle competenze nei settori regolati dalla direttiva NIS2;
- Ridurre il divario di genere: oggi le donne rappresentano solo il 19% degli specialisti ICT;
- Avviare programmi specifici sulla sicurezza dell'intelligenza artificiale e sulla crittografia resistente ai futuri computer quantistici.

Tuttavia, ENISA sottolinea che colmare il gap di competenze richiede una collaborazione senza precedenti. L'agenzia propone la creazione di un *Fondo Europeo per la formazione in Cybersecurity* da 200 milioni di euro; stabilire regole per garantire un numero minimo di esperti nelle infrastrutture critiche; semplificare l'ingresso in Europa di talenti internazionali attraverso

visti agevolati. Senza queste misure, l'Europa rischia di perdere terreno nella corsa globale alla resilienza digitale.