

Colmare il Divario: Affrontare la carenza di competenze nella Cybersecurity

La rapida evoluzione delle tecnologie digitali si accompagna ad una crescente domanda globale di esperti in sicurezza informatica. Tuttavia, le aziende fanno fatica a trovare figure professionali qualificate: oltre la metà di chi cerca personale in questo settore incontra difficoltà nel processo di selezione. Se il 45% lamenta una carenza di candidati preparati, il 44% segnala una mancanza generale di persone interessate. A questi problemi si aggiungono la scarsa conoscenza delle opportunità nel settore (22%) e i limiti di budget (16%).

Questa carenza di talenti rappresenta un rischio critico per aziende e organizzazioni, se consideriamo che le minacce informatiche sono sempre più sofisticate e frequenti. Senza un numero sufficiente di professionisti in grado di proteggere dati e infrastrutture digitali, aumenta la vulnerabilità ad attacchi informatici, violazione di dati e interruzioni operative. Il problema, quindi, non è solo occupazionale, ma riguarda la sicurezza stessa del mondo digitale.

Affrontare questa sfida richiede un approccio multifattoriale. Innanzitutto, è fondamentale investire nella formazione: creare percorsi educativi, corsi professionali e programmi di certificazione per preparare nuove generazioni di esperti. Le collaborazioni tra pubblico e privato possono facilitare questo processo, ad esempio finanziando borse di studio, stage e apprendistati per attirare nuovi talenti nel settore. Inoltre, iniziative di riqualificazione e aggiornamento professionale rivolte a lavoratori provenienti da ambiti affini, come l'IT e l'ingegneria, possono contribuire ad ampliare il bacino di talenti.

Sono anche necessarie campagne di sensibilizzazione per mettere in luce le opportunità di carriera redditizie offerte dalla cybersecurity. Molti candidati, infatti, ignorano si tratti di un settore in forte crescita, con buone prospettive di carriera e un impatto concreto sulla società. Promuovendo la cybersecurity come un percorso di carriera accessibile e gratificante, le organizzazioni possono attrarre una forza lavoro più diversificata, includendo gruppi sottorappresentati come donne e minoranze.

Le aziende, dal canto loro, devono rivedere le proprie strategie di assunzione per adattarsi alla realtà del mercato del lavoro. Dare maggiore peso all'esperienza pratica e alle certificazioni, anziché limitarsi ai titoli accademici tradizionali, può aprire le porte a profili interessanti che altrimenti verrebbero esclusi. Promuovere e favorire una cultura aziendale basata sull'apprendimento continuo è altrettanto cruciale per garantire che i dipendenti attuali restino aggiornati sugli ultimi sviluppi in materia di cybersecurity.

In definitiva, colmare il divario di competenze nella cybersecurity richiede uno sforzo congiunto tra istituzioni, scuole, università e imprese. Solo creando un ecosistema inclusivo e dinamico, capace di formare professionisti competenti e motivati, sarà possibile rispondere alle crescenti sfide della sicurezza digitale.

Un esempio concreto in questa direzione è **CyberPro Train**, un'iniziativa pensata per affrontare il cuore del problema. Attraverso percorsi formativi strutturati, il coinvolgimento di leader del settore e risorse educative mirate, CyberPro Train contribuisce in modo attivo alla creazione di una forza lavoro preparata e resiliente, assicurando che aziende e istituzioni possano contare sui professionisti qualificati di cui hanno bisogno per proteggere i propri asset digitali.

Fonte:

<https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home>,
<https://europa.eu/eurobarometer/surveys/detail/3176>