ARTICOLO DI ELEARNINGNEWS

Anno 10 - numero 365 di Mercoledì 04 febbraio 2026

Cybersicurezza e difesa: la formazione come priorità europea

Dagli incontri istituzionali a Bruxelles con Commissione Europea e NATO emerge un messaggio chiaro: la cybersicurezza è parte integrante della difesa europea e la formazione del personale rappresenta il primo fattore di resilienza per imprese e istituzion

Negli ultimi anni la cybersicurezza ha progressivamente superato i confini della dimensione tecnica per affermarsi come uno dei pilastri della sicurezza strategica europea. La protezione dei sistemi informativi, delle infrastrutture critiche e dei dati non rappresenta più soltanto un'esigenza operativa per le singole organizzazioni, ma una condizione essenziale per la stabilità economica, sociale e istituzionale dell'Unione Europea.

Questa consapevolezza è emersa con particolare forza in occasione della tavola rotonda europea sul digital skill gap, organizzata da DIGITALEUROPE nel contesto del Digital Skills Summit 2025. L'incontro, cui ha partecipato anche il bresciano **Luigi Matteo Meroni, CEO di Mega Italia Media**, si è svolto alla presenza della Vicepresidente Esecutiva della Commissione Europea Roxana Mînzatu.

Tra gli intervenuti, anche il **Segretario Generale della NATO**, che ha ribadito la necessità di creare una cultura della difesa e di rafforzare le competenze digitali delle aziende.

Dal cybercrime alla cyberwar: il cambiamento della minaccia

Uno degli aspetti più rilevanti emersi riguarda la profonda trasformazione della natura degli attacchi informatici. Per lungo tempo, il cybercrime è stato prevalentemente associato ad attività criminali finalizzate al profitto economico: furti di dati, estorsioni, frodi informatiche, **ransomware**. Oggi questo scenario risulta incompleto e, per certi versi, superato.

Gli attacchi informatici stanno sempre più assumendo le caratteristiche di **azioni ostili coordinate**, riconducibili a strategie di pressione geopolitica e di destabilizzazione sistemica. Non si tratta più soltanto di colpire singole aziende, ma di compromettere infrastrutture critiche, servizi essenziali e catene del valore strategiche a livello europeo.

Reti energetiche, sistemi di trasporto, sanità, telecomunicazioni, pubbliche amministrazioni e grandi gruppi industriali rappresentano obiettivi sensibili, il cui malfunzionamento può produrre effetti a cascata sull'intera società. In questo contesto, il cyberspazio diventa un vero e proprio **dominio operativo**, al pari di quelli terrestre, marittimo, aereo e spaziale.

Il messaggio è chiaro: l'Unione Europea non è soltanto esposta a rischi tecnologici, ma a **minacce ibride**, in cui il digitale viene utilizzato come strumento di pressione politica, economica e strategica.

Il fattore umano come perimetro della sicurezza

In un contesto di minacce sempre più sofisticate, il perimetro della sicurezza non può più essere identificato esclusivamente con le infrastrutture tecnologiche. Firewall, sistemi di monitoraggio e **soluzioni di cybersecurity avanzate** rappresentano strumenti indispensabili, ma non sufficienti.

Il **fattore umano** rimane il principale vettore di attacco e, allo stesso tempo, il primo presidio di difesa. Phishing, social engineering, compromissione delle credenziali e utilizzo improprio degli strumenti digitali continuano a essere tra le principali cause di incidenti di sicurezza.

Un'analogia efficace è quella della sicurezza sul lavoro: non basta disporre di macchinari sicuri se le persone non sono formate a utilizzarli correttamente. Allo stesso modo, nel dominio digitale, la sicurezza non è garantita dalla tecnologia in sé, ma dal

comportamento consapevole di chi la utilizza.

Formare il personale significa quindi **ridurre la superficie di attacco**, aumentare la capacità di riconoscere situazioni anomale e trasformare ogni lavoratore in un soggetto attivo della difesa digitale dell'organizzazione.

Il gap formativo europeo: una vulnerabilità sistemica

Il 70% delle aziende europee non ha programmi strutturati di formazione in materia di cybersicurezza.

L'assenza di formazione diffusa genera una vulnerabilità sistemica che coinvolge intere filiere produttive e reti di fornitura. In un'economia fortemente interconnessa, la sicurezza di un'organizzazione dipende anche dal livello di maturità cyber dei propri partner, fornitori e collaboratori.

Questo fenomeno assume particolare rilevanza alla luce delle più recenti normative europee, che pongono un forte accento sulla gestione del rischio lungo l'intera catena del valore. La mancanza di competenze diffuse non rappresenta solo un problema operativo, ma un fattore di rischio strategico per la competitività e la resilienza del sistema economico europeo.

Formazione sulla Cyber Security: dalla compliance alla resilienza

Le istituzioni europee hanno avviato negli ultimi anni un percorso normativo ambizioso, volto a rafforzare il livello complessivo di sicurezza digitale. La **Direttiva NIS2**, ad esempio, introduce obblighi più stringenti in materia di gestione del rischio, governance e formazione del personale, riconoscendo esplicitamente il ruolo centrale delle competenze.

In questo contesto, la formazione non deve essere interpretata come un mero adempimento formale, ma come una **leva strategica di resilienza organizzativa**. Un'organizzazione formata è in grado di prevenire incidenti, ridurre i tempi di risposta, limitare i danni e garantire la continuità operativa anche in scenari di crisi.

La formazione continua consente inoltre di adattarsi a un panorama di minacce in costante evoluzione, superando l'approccio statico e puntando su un modello dinamico di sicurezza, basato sull'aggiornamento costante delle competenze.

Il contributo di Mega Italia Media alla cultura della Cyber Sicurezza

In questo scenario complesso, la formazione assume il valore di una vera e propria **infrastruttura immateriale di difesa**. Mega Italia Media, attraverso la propria offerta formativa dedicata alla sicurezza informatica, contribuisce a rispondere in modo concreto a un'esigenza chiaramente identificata a livello europeo e internazionale.

L'obiettivo non è soltanto trasferire conoscenze tecniche, ma promuovere una **cultura della cybersicurezza**, capace di incidere sui comportamenti quotidiani delle persone e sulle scelte strategiche delle organizzazioni. Una cultura che riconosce nella formazione uno strumento essenziale per colmare il gap di competenze e rafforzare la resilienza del sistema produttivo.

Come emerso anche dagli incontri istituzionali a Bruxelles, investire in formazione significa investire nella sicurezza collettiva, contribuendo alla stabilità e alla competitività dell'Europa nel lungo periodo.

Visita questa pagina e scopri tutti i corsi sulla Cybersecurity di Mega Italia Media.

La cybersicurezza non può più essere considerata un tema settoriale o delegabile. È una responsabilità condivisa che coinvolge istituzioni, imprese e singoli individui. Costruire una cultura della difesa digitale significa riconoscere che ogni comportamento conta e che la formazione rappresenta il primo e più efficace strumento di prevenzione.

In un contesto in cui il cyberspazio è diventato un dominio strategico, la consapevolezza e le competenze delle persone costituiscono la linea di difesa più avanzata.