Le Pmi di fronte alla sfida della nuova normativa Ue sulla cybersicurezza

Andrea Marini

Le piccole e medie imprese sono pronte ai nuovi adempimenti sulla cybersicurezza, in applicazione della nuova direttiva europea NIS 2. Timori ancora sussistono, ma cresce la consapevolezza che, di fronte allo sviluppo delle tecnologie digitali, misure come l'analisi del rischio e la gestione degli incidenti sono un fattore sempre più importante per la competitività. Le aziende però chiedono un aiuto alle associazioni di categoria e alle istituzioni, che dal loro punto di vista si dicono disponibili a fornire assistenza. Di questo si è parlato ieri a Roma, al Centro Studi Americani, in un roadshow organizzato da Tim Enterprise e Unindustria Lazio.

«Nel Lazio operano il 22% di tutte le aziende italiane della cybersicurezza che impiegano circa 5.500 addetti (18,8% del totale nazionale)», ha spiegato Giuseppe Biazzo, presidente di Unindustria Lazio. Per una azienda «l'adeguamento alla NIS 2 – ha aggiunto – può diventare un volano per rafforzare la propria resilienza cibernetica, migliorare l'immagine e incrementare la competitività».

Eugenio Santagata, Chief Public Affairs, Security & International Business di TIM, Chairman e CEO di Telsy, ha evidenziato l'importanza della collaborazione tra pubblico e privato, aggiungendo: «Ogni giorno un pezzo di economia e società diventa digitale, facendo così crescere i punti deboli». Secondo i dati raccolti dal Centro Studi TIM, il 61% delle piccole e medie imprese si ritiene bersaglio di attacchi informatici, ma solo il 32% si ritiene pronto a gestirli. Nel 2023 i soggetti target di attacchi informatici sono cresciuti del 187%.

Bruno Frattasi, direttore dell'Agenzia per la cybersicurezza, ha voluto rassicurare: «La normativa sarà applicata in Italia in maniera graduale. La nostra Agenzia è a disposizione di imprese e pubblica amministrazione per fornire supporto. Non dobbiamo essere spaventati».

La normativa (entrata in vigore ieri in Italia e con una serie di adempimenti per le imprese a partire dall'anno prossimo) è molto stringente: «L'ambito di applicazione oscilla tra le 30mila e le 50mila aziende», ha spiegato Lorenzo Benigni, vicepresidente con delega alla cybersecurity di Unindustria Lazio, che poi ha aggiunto: «Il Lazio è un territorio delicato da proteggere, visto che comprende la maggior parte delle istituzioni, nonché degli enti della difesa».

Cristiano Dionisi (SICOI), presidente della Piccola Industria Unindustria Lazio, ha parlato della necessità che le istituzioni definiscano «linee guida più precise possibili. Occorre fare rete sia a livello di filiere che di territori per aiutare le piccole imprese a rispettare gli obblighi». Roberta Angelilli, vicepresidente e assessore allo Sviluppo della Regione Lazio, ha chiesto di «fare sistema» per facilitare i nuovi obblighi. «Servono risorse – ha aggiunto – confidiamo nella nuova Commissione Ue». Massimo Scaccabarozzi (Menarini Biotech), presidente Sezione Farmaceutica di Unindustria, ha sottolineato l'importasnza per il suo settore della cyber sicurezza: «C'è il problema dello spionaggio. Per noi è strategico avere protezione, fin dalla ricerca». Per Maddalena Nocivelli (DAB Sistemi Integrati), presidente sezione IT Unindustria Lazio, occorre essere «concreti e pratici. Unindustria può dare supporto alle aziende», mentre Francesca Basilico (San Raffaele), presidente Sezione Sanità di Unindustria, ha concluso che tutte le aziende del comparto «hanno iniziato ad applicare le nuove procedure, anche se sono emerse criticità, come nei pronto soccorso».