

Cisco, le aziende italiane impreparate sulla cybersecurity



In Italia soltanto il 7% delle aziende è in grado di difendersi dalle minacce informatiche rispetto al 15% a livello globale. A lanciare l'allarme è il Cybersecurity Readiness Index 2023, il rapporto realizzato da Cisco in 27 paesi del mondo su un campione di 6.700 professionisti che operano in quest'ambito, per misurare la preparazione e la resilienza delle aziende nei confronti della criminalità informatica. Il 75% degli intervistati si aspetta nei prossimi 12-24 mesi un'interruzione della propria attività a causa di un attacco informatico, mentre il 31% ha dichiarato di averne subito uno nel corso dell'ultimo anno. Il report quantifica anche il costo degli attacchi: il 25% delle aziende colpite, a livello globale, ha dovuto spendere almeno 500.000 dollari (circa 456.000 euro) per riprendere il controllo della propria

attività. “Sta emergendo nelle realtà italiane una maggiore sensibilità e consapevolezza sul tema della cybersecurity, che è entrato nelle discussioni del board”, commenta Andrea Castellano, Cybersecurity Leader Cisco Italia, sottolineando che il 94% degli intervistati dichiara di voler investire in infrastrutture It per rafforzare la propria posizione sulla sicurezza informatica. Inoltre, l’87% prevede di aumentare il proprio budget per la sicurezza di almeno il 10% nei prossimi 12 mesi. “L’errore più grande da parte delle aziende è quello di difendersi dagli attacchi informatici utilizzando un mix di strumenti”, spiega Jeetu Patel, executive vice president and general manager of security and collaboration at Cisco. “Occorre invece considerare piattaforme integrate, grazie alle quali le aziende possono raggiungere un grado di resilienza sufficiente colmando allo stesso tempo il loro gap di preparazione nei confronti della cybersecurity.” Per realizzare il Cisco Cybersecurity Readiness Index 2023 sono stati presi in considerazione i cinque pilastri fondamentali della cybersecurity: l’identità, i dispositivi, la sicurezza della rete, i carichi di lavoro applicativi, i dati. Ciascuno di essi comprende a sua volta 19 diverse soluzioni. Al termine dell’indagine le aziende sono state classificate in quattro gradi di preparazione: principiante, formativo, progressivo, maturo. In Italia, se il 7% delle aziende è nella fase matura, l’8% si trova ancora in quella principiante e il 61% in quella formativa: una preparazione in materia di cybersecurity molto inferiore alla media.