24-NOV-2025
da pag. 6 / foglio 1

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 54208 Diffusione: 113068 Lettori: 657000 (Data Stampa 0006901)

L'intervista

Andrea Monti

«Agevolazioni pubbliche più efficaci per le Pmi»

«Oggi sono attive diverse misure pubbliche e le risorse stanziate testimoniano l'impegno con cui si sta sostenendo la trasformazione digitale del Paese. Per accompagnare al meglio le Pmi in questo percorso, sarà importante continuare a rafforzare strumenti sempre più strutturali, mirati e flessibili: misure con requisiti proporzionati, liste di beni aggiornate alle esigenze reali – dall'Ai alla cybersecurity – e procedure stabili, così da dare continuità agli investimenti, ormai fondamentali per la competitività. Un impegno che vede coinvolte sia le istituzioni sia realtà come la nostra, che ogni giorno affiancano le aziende nel rafforzamento della loro protezione digitale». Così il direttore generale di Tinexta Cyber, Andrea Monti, che in questa intervista affronta il costante aumento degli attacchi informatici. «Ogni semestre - dice - registriamo un incremento».

Il problema è che le infrastrutture di sicurezza informatica hanno un costo, molto spesso salato.

La parola "costo" non mi convince. Preferisco parlare di investimento in cybersicurezza, perché lo paragono a un'assicurazione o a un antifurto. Ha un effetto deterrente e allo stesso tempo garantisce una protezione necessaria. E, devo dirlo, parliamo comunque di un esborso minimo se confrontato con il danno potenziale che può seguire a un attacco. Il vero problema, oggi, è la percezione: si pensa ancora che certi eventi siano rari. Si sottovaluta l'impatto possibile, che non è solo reputazionale. È in gioco la continuità stessa del business, con il rischio concreto che, in caso di blocco produttivo dovuto a un attacco, i clienti si rivolgano ai concorrenti.

Si tratta di attacchi complessi?

C'è un dato che da solo rende l'idea di cosa stiamo parlando. Circa il 70% degli attacchi andati a segno sfrutta vulnerabilità talmente note che basterebbe un'infrastruttura di cybersicurezza base per bloccarli. Si tratta di falle elementari che restano aperte. E il rischio è tutt'altro che teorico: secondo alcune stime, sul dark web circolano oltre 15 miliardi di credenziali di accesso ai sistemi aziendali, a livello globale. Questo significa che per molti criminali informatici non è nemmeno necessario "bucare" un sistema: possono semplicemente comprare un pacchetto di username e password già pronte e provarle in serie, con un costo minimo e un potenziale impatto enorme per le imprese.


Cybersicurezza: incentivi a metà fra burocrazia e spese escluse