24-MAG-2025
da pag. 8 / foglio 1

Il Sole 24 ORE
Quotidiano - Dir. Resp.: Fabio Tamburini
Tiratura: 60126 Diffusione: 116170 Lettori: 675000 (DS0006489)

La guerra invisibile tra hacker, spioni e sovranità digitale

Nel panel Emilio Gisondi, Silvio Ranise, Yuri Giuseppe Rassega, Fabio Scacciavillani, Giovanni Andrea Toselli

Cybersecurity

Gli esperti: «Le minacce digitali crescono più in fretta delle nostre difese»

Andrea Biondi
Dal nostro inviato
TRENTO

Nel mondo delle guerre ibride, dove non si spara ma si clicca, la cybersecurity è un dossier strategico. Al Festival dell'Economia di Trento, il panel "Cybersecurity: spie, spioni e hacker" ha posto al centro del dibattito la necessità di un cambio di passo: non è più solo un tema tecnico, ma questione di sicurezza nazionale, economica e democratica.

«Siamo come Davide contro Golia» è la metafora usata da Silvio Ranise, direttore del Centro di Cybersecurity della Fondazione Bruno Kessler. «L'attaccante ha più vantaggi del difensore» e oggi l'intelligenza artificiale ha reso l'aggressione più semplice, più personalizzata, più subdola, spiega Ranise. È il rovescio oscuro dell'innovazione: la macchina che scrive phishing credibili, come se ci conoscesse. Perché, in fondo, ci conosce.

A ogni modo si tratta, ha ricordato Emilio Gisondi di Tinexta Defence nel corso del panel moderato da Simone Casalini, direttore di Il T Quotidiano, di una questione che riguarda la sovranità: «Non possiamo continuare a dipendere da tecnologie estere, anche se alleate». Un'affermazione forte, che richiama il concetto – antico, ma oggi centrale – di indipendenza strategica.

Il salto da fare, però, è anche culturale. Lo ha spiegato bene Yuri Giuseppe Rassega, a capo della cybersecurity di Enel. «Non siamo più nell'epoca dell'hacker solitario. Oggi chi attacca è un'organizzazione fluida, globale, senza regole e con grandi mezzi». Ecco che da fatto eccezionale la cibersicurezza deve trasformarsi in capitolo ordinario.

E poi ci sono i numeri, eloquenti. Fabio Scacciavillani, socio fondatore e strategist di Nextperience li snocciola: 500mila attacchi al giorno su Poste Italiane. Il valore annuale delle attività di hacking cinesi? Ben 650 miliardi di dollari. E soprattutto: «In America, l'80% delle vittime si accorge di essere stata colpita solo quando arriva la polizia».

Oggi comunque «c'è più attenzione, ma resta il divario tra grandi imprese e Pmi. E questo è un problema di sistema» sottolinea Giovanni Andrea Toselli, ceo di PwC Italia. Ecco allora il vero punto: serve una consapevolezza collettiva. Un'alfabetizzazione digitale diffusa. Anche perché non si tratta neanche più solo di furti di dati. C'è tutto il tema della disinformazione sistematica, manipolazione dell'opinione pubblica attraverso i social. È la "guerra ibrida". «Dobbiamo fare i compiti a casa», conclude Ranise. Un'espressione che richiama qualcosa di scolastico. Ma che qui suona come una convocazione alla responsabilità.