IL SOLE 24 ORE – 23 MARZO 2026

«L’obiettivo è avere più tutele senza frenare le aziende»

intervista a Marnix Dekker, di Margherita Ceci

La necessità di difendersi da un lato, e quella di essere competitivi dall’altro: «Quando si fanno le normative bisogna tenere conto di queste due esigenze», spiega Marnix Dekker, vicecapo dell’unità per la resilienza dei settori critici dell’Enisa. «Abbiamo creato molte regole in Europa, che a volte ostacolano le aziende, specialmente se sono diverse nei singoli Paesi. Questa proposta, oltre a rafforzare la sicurezza di tutto l’ecosistema digitale, armonizza».

In che modo?

«Introducendo per esempio una certificazione cyber trasversale sull’azienda stessa, non solo sui servizi che offre, come accade attualmente. La certificazione sarebbe uguale per tutti Paesi e aiuterebbe le aziende a lavorare facilmente in più Stati, semplificando al tempo stesso il lavoro dell autorità nella supervisione dei settori critici sotto la Nis2»

La valutazione della supply chain e dei Paesi terzi non produrrà l’effetto opposto?

«Bisogna capire il contesto: l’It non è più quella di una volta, un sistema chiuso gestito internamente all’azienda. Ora è tutto basato sul cloud, sempre connesso e gestito da terzi, i managed service providers. Servono aggiornamenti giornalieri, già con un piccolo ritardo si è a rischio. Per questo si delega sempre più a fornitori esterni la configurazione e la gestione dei prodotti. Le responsabilità e i compiti di sicurezza si spostano su questi soggetti: da qui il problema della sovranità. Da dove arriva l’It e chi lo gestisce? Chi ha accesso ai dati? È un Paese di cui ti puoi fidare?».

Non è un tema nuovo.

«Nelle telecomunicazioni è diventato un problema con il passaggio dal 4G al 5G. È un settore critico, con dati importanti. Qualche anno fa è stato sviluppato a livello europeo il 5G Toolbox, una linea guida per gestire nuovi rischi, ma l'adozione era volontaria: alcuni Paesi hanno fatto tanto, altri meno, in una situazione di disparità. Con la nuova proposta l'Ue introduce un sistema per gestire quei rischi non tecnici provenienti dai fornitori nei Paesi a rischio, come la Cina, includendo tutti settori, non solo telecomunicazioni».

Quali minacce dobbiamo aspettarci prossimamente?

«Un po' di tutto, come stiamo già vedendo da anni: si va dal ransomware alle minacce ibride e allo spionaggio da parte di gruppi legati agli Stati. Le capacità degli aggressori continuano a migliorare, diventano sempre più veloci e ora sono anche supportate dall'Ai. Prendono di mira infrastrutture critiche, aziende, governi centrali, ma anche Comuni, politici, giornalisti... Tanti attacchi iniziano ancora con un email. L'abbiamo visto anche agli inizi della guerra iraniana: un gruppo russo ha usato dei messaggi che davano informazioni sulla guerra per riuscire a infiltrarsi nei sistemi».